



# **Strategic Cloud Adoption in Financial Services: Governing Risk & Scaling RegTech**



**REPORT – SEPTEMBER 2026**

**KPMG & SFA**

## Table of Contents

|                                                                            |    |
|----------------------------------------------------------------------------|----|
| Foreword .....                                                             | 2  |
| Overview & Report Structure .....                                          | 3  |
| Acknowledgements .....                                                     | 5  |
| Executive Summary .....                                                    | 7  |
| Overview .....                                                             | 7  |
| Key Next Steps- FIs, SIs, CSPs and RegTechs .....                          | 8  |
| Glossary of Terms .....                                                    | 9  |
| Chapter 1: RegTech Evolution & the Cloud Imperative .....                  | 10 |
| MAS Insights .....                                                         | 12 |
| Key Takeaways .....                                                        | 12 |
| Chapter 2: Cloud Security & Shared Responsibility .....                    | 13 |
| Illustrative Common Operating Model for Cloud-Based RegTech Adoption ..... | 16 |
| MAS Insights .....                                                         | 17 |
| Key Takeaways & Next Steps .....                                           | 18 |
| Chapter 3: Data Sovereignty, Privacy & Regulatory Compliance .....         | 19 |
| Key Takeaways and Next Steps .....                                         | 20 |
| Chapter 4: Risk Management, Governance & Operational Resilience .....      | 22 |
| MAS Insights .....                                                         | 23 |
| Key Takeaways and Next Steps .....                                         | 24 |
| Chapter 5: Strategic Value & Business Case for Cloud-Based RegTech .....   | 25 |
| Key Takeaways .....                                                        | 26 |
| Conclusion .....                                                           | 27 |

## Foreword

The financial services industry is entering a new phase of technology adoption. Cloud has moved well beyond being an infrastructure choice. It is now an important part of how financial institutions modernise regulatory and compliance functions, improve resilience, make better use of data and adopt new capabilities such as AI.

For Singapore's financial ecosystem, there is a clear opportunity. Cloud-based RegTech can help financial institutions respond more effectively to growing regulatory complexity and give them access to capabilities that may be difficult or costly to build and maintain on their own. But getting value from these solutions also depends on how they are governed and managed, particularly as financial institutions rely on a growing number of technology and service providers.

This report brings together perspectives from Financial Institutions, RegTech providers, Cloud Service Providers, System Integrators and the Monetary Authority of Singapore (MAS). This is important because the challenges around cloud adoption rarely sit with one party alone. Regulators, financial institutions and technology providers each see different parts of the picture, and progress depends on bringing those perspectives together.

There is also no single model that will work for every institution or use case. A risk-based approach will be important, allowing institutions to make use of cloud in ways that reflect the specific use case and risks involved, while maintaining the standards of resilience and trust expected of Singapore's financial sector.

At the Singapore FinTech Association (SFA), we see collaboration as an important part of the next phase of cloud adoption. Financial institutions are increasingly working with a broader range of technology partners, which means responsibilities and risks are also shared across more parties. Greater clarity around roles and accountability, together with more practical and consistent approaches to areas such as data governance, third-party risk and operational resilience, will help the industry adopt cloud-based RegTech with greater confidence.

I hope this report serves as a practical reference for industry participants and helps move the conversation from what cloud-based RegTech can do, to how we can adopt it well. If we can continue to build trust, strengthen capabilities and work through the practical barriers to adoption, Singapore will be well placed to remain a leading centre for responsible financial innovation.

**Holly Fang**

President

Singapore FinTech Association



# Overview & Report Structure

The **Singapore Fintech Association (SFA)** and **KPMG** conducted the following key activities to capture strategic insights across an ecosystem of sector players on cloud-enabled RegTech adoption:

- 1 A series of industry workshops with **RegTechs, Cloud Service Providers (CSPs), and Financial Institutions (FIs)**;
- 2 A targeted survey across **17 RegTech providers**;
- 3 Targeted questionnaire-based interviews with **System Integrators (SIs)** on their role in cloud-enabled RegTech adoption;
- 4 A targeted questionnaire-based interview with the **Monetary Authority of Singapore (MAS)** to capture supervisory insights across key areas impacting cloud-enabled RegTech adoption.

Collectively, the insights outlined in this report provide practical thought leadership on the secure adoption of cloud-based RegTech solutions. The report addresses critical cloud security considerations for FIs deploying RegTech solutions in Singapore and across the Asia-Pacific region, while also tackling ongoing security and compliance challenges. Furthermore, it proposes a common framework to help FIs harness innovative RegTech capabilities while maintaining strong security and risk management practices.

## Coverage Areas and Chapter Scope

This report reflects the aggregated views and perspectives of the participating institutions identified above. Its purpose is to highlight common themes and key considerations associated with cloud adoption. For the avoidance of doubt, the information contained herein does not constitute regulatory guidance and should not be construed as prescriptive guidance, regulatory requirements, or expectations for industry participants.

While common themes have been identified, these reflect **industry viewpoints rather than uniform consensus**, with variations **observed across stakeholder groups**. The details provided in this report highlight outcomes across five key chapters, as outlined below:

| Chapter | Topic                                                   |
|---------|---------------------------------------------------------|
| 1       | RegTech Evolution and the Cloud Imperative              |
| 2       | Cloud Security Framework for RegTech Solutions          |
| 3       | Data Sovereignty, Privacy & Regulatory Compliance       |
| 4       | Risk Management, Governance & Operational Resilience    |
| 5       | Strategic Value & Business Case for Cloud-Based RegTech |

A summary of each chapter is provided below:



## **Report Structure**

Across all chapters, the report content has been directly shaped by structured, guided questions posed during the workshops, questionnaires, and surveys, which captured practical perspectives from FIs, SIs, RegTechs, and CSPs on key challenges spanning cloud adoption, security, data governance, risk management, and strategic value.

This report includes chapter-specific summaries based on the outcomes of workshops and questionnaires conducted from April to June 2026 with RegTechs, CSPs, FIs, SIs, and MAS, where relevant. This includes the following:

- **Summary of areas of common alignment and key considerations- Split by FIs, SIs, RegTechs and CSPs**
- **MAS Insights (*where applicable*)**
- **Key Takeaways and Next Steps (*where applicable*)**

## Acknowledgements

This report was developed in collaboration with the Singapore FinTech Association (SFA), KPMG Singapore, and the SFA RegTech Subcommittee. It reflects the valuable inputs and contributions from FIs, CSPs, SIs and RegTechs, as well as representatives from the MAS.

We extend our sincere appreciation to all stakeholders for their valuable perspectives and contributions, which have been instrumental in shaping a balanced and ecosystem-driven view of cloud adoption and operational resilience across the industry.

|                                 |                                                                                                                                                                                                                                                                                                                         |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SFA</b>                      | <ul style="list-style-type: none"><li>• <b>Bryan Tay</b>, General Manager</li><li>• <b>Samantha Soong</b>, Program Lead, Subcommittees &amp; Working Groups</li></ul>                                                                                                                                                   |
| <b>SFA RegTech Subcommittee</b> | <ul style="list-style-type: none"><li>• <b>Kew Yoke Ling</b>, Executive Director, Kewmann and Subcommittee Chair</li><li>• <b>Julia Chin</b>, CEO, JFourth Solutions</li><li>• <b>Rolf Haudenschild</b>, Head of Regulatory Compliance Services, Alpadis</li><li>• <b>Jacqueline Pang</b>, CEO, Artius Global</li></ul> |

*A special thanks to Florian Dumas, Executive Director, U-Reg & former Subcommittee Chair for informing the idea for this report.*

|                       |                                                                                                                                                                                                                                                 |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>KPMG Singapore</b> | <ul style="list-style-type: none"><li>• <b>Sinchan Banerjee</b>, Partner, Financial Services Consulting</li><li>• <b>Wendy Lim</b>, Partner, Cyber</li><li>• <b>Inoue Quartier</b>, Associate Director, Financial Services Consulting</li></ul> |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Workshop, Interview & Survey Participants:

|                                        |                                                                                             |
|----------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Monetary Authority of Singapore</b> | <ul style="list-style-type: none"><li>• <b>Kenneth Gay</b>, Chief FinTech Officer</li></ul> |
|----------------------------------------|---------------------------------------------------------------------------------------------|

|             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>CSPs</b> | <ul style="list-style-type: none"><li>• <b>AWS</b>- Matt Nixon, Principal - Financial Services Cloud Risk, Security, and Compliance Specialist; Brenda Fong, Senior FSI Risk and Compliance Specialist</li><li>• <b>Google Cloud</b>- Michalis Tsavdaridis, Head of Cloud CISO - Security, Risk &amp; Compliance - JAPAC &amp; META; Luka Debeljak Director, Customer Engineering, Southeast Asia</li><li>• <b>Huawei Cloud</b>- Dennis Chan, Chief Security Officer</li><li>• <b>Microsoft Azure</b>- Eugene Teo, Chief Security Officer</li><li>• <b>Oracle Cloud</b>- Roshan Navendra, Chief Customer Architect; David Warnowidodo, Director - Security &amp; Manageability Cloud Specialists, Asia Pacific; Danish Choo, Sales Manager (Data, AI &amp; Infrastructure)</li><li>• <b>Tencent Cloud</b>- Harry Zheng, Senior Solution Architect</li></ul> |
| <b>FIs</b>  | <ul style="list-style-type: none"><li>• <b>ADDX</b>- Lyndon Seow, Head, Group Legal &amp; Compliance</li><li>• <b>ANEXT Bank</b>- Jackson Oh, Chief Technology Officer</li><li>• <b>Atlas Consolidated</b>- Braham Djidjelli, Co-Founder and Chief Product Officer; Surya Chaitanya Tamada, Co-Founder</li><li>• <b>Corecam Pte. Ltd</b>- David Doerig, Managing Partner - Chief Operating Officer</li><li>• <b>Eightstone</b>- Chiara Bartoletti, Managing Partner, Chief Operating Officer</li><li>• <b>Lighthouse Canton</b>- Willie Ong, Executive Director, Compliance</li><li>• <b>LMAX</b>- Geetanjali Desai, Head of Compliance</li><li>• <b>StraitsX</b>- Victor Liew, Co-Founder &amp; Chief Technology Officer</li><li>• <b>Wise</b>- Lim Kiat, Engineering Lead, APAC</li></ul>                                                                 |

|                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RegTechs</b> | <ul style="list-style-type: none"> <li>• <b>Flagright</b>- Baran Ozkan, CEO</li> <li>• <b>Hawk.ai</b>- Brendan Choo, Regional Account Director, APAC</li> <li>• <b>Kewmann</b>- Kew Yoke Ling, Executive Director</li> <li>• <b>LexisNexis Risk Solutions</b>- Marlene Vicaire, Senior Director, Market Planning – Fraud &amp; Identity, APAC</li> <li>• <b>MyComplianceOffice</b>- Kelly-Ann McHugh, Director, Asia Pacific</li> <li>• <b>Sumsub</b>- Darren Yan, APAC Partnership Director</li> <li>• <b>Zavior</b>- Glenn Tan, CEO</li> </ul> |
| <b>SIs</b>      | <ul style="list-style-type: none"> <li>• <b>NCS</b>- Balaji Mohan, Practice Lead for Cyber AI Security &amp; Threat Defense</li> <li>• <b>System Asia</b>- Willam Wu, Service Sales Manager</li> </ul>                                                                                                                                                                                                                                                                                                                                           |

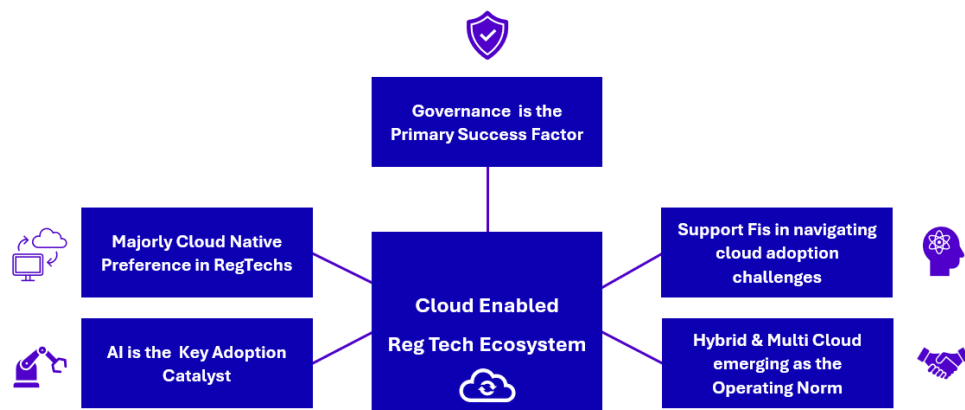
# Executive Summary

## Overview

Cloud has emerged as a non-discretionary capability for FIs, underpinning AI adoption, advanced analytics, and the continued evolution of RegTech. Cloud is now a strategic enabler of RegTech transformation. Its role has shifted from an infrastructure choice to an enabler of scalability, resilience, interoperability, and regulatory agility, with hybrid and multi-cloud architectures increasingly becoming the prevailing model.

While adoption is accelerating, particularly among small and mid-sized FIs, progress remains uneven. The primary constraints are no longer mainly technological, but operational: translating principle-based regulatory expectations into consistent, day-to-day practices remains a key challenge. Capability gaps, legacy technology constraints, and complexities around data sovereignty, privacy, and cross-border compliance continue to affect the pace of scaled adoption.

The report highlights that cloud-enabled RegTech operates within a complex, multi-party ecosystem spanning FIs, RegTech providers, CSPs, SIs, and other third parties. As responsibilities become increasingly distributed, traditional ownership models are no longer sufficient. There is a clear need for a more coordinated, ecosystem-led approach anchored in well-defined accountability, federated governance structures, standardised assurance practices, and shared implementation artefacts. Structural risks including concentration risk, data privacy risks, third-party dependencies, and emerging AI-related risks must be actively managed on a collective basis rather than addressed in isolation.



At the same time, the value proposition of cloud is evolving beyond cost efficiency toward strategic outcomes, including improved resilience, faster regulatory responsiveness, and enhanced access to AI capabilities. AI is accelerating adoption and creating new opportunities across KYC, AML, fraud, monitoring, and reporting. However, both FIs and ecosystem participants continue to face challenges in consistently articulating and measuring these benefits. Survey findings from 17 Singapore-based RegTechs reinforce this disconnect: while 77% favour cloud-native deployment models, 94% report encountering FI hesitancy toward cloud adoption. Despite a more distributed ecosystem, accountability remains with the FI, including governance, oversight, risk management, and incident response. This misalignment underscores the need for stronger assurance frameworks, standardisation, clearer articulation of shared responsibilities, and increased reliance on hybrid deployment models.

MAS remains supportive of both cloud adoption and RegTech innovation, highlighting that meaningful progress has been made in established use cases such as transaction monitoring, sanctions screening, and regulatory reporting. However, MAS has further emphasised the need to progress toward more integrated, end-to-end compliance solutions spanning the full lifecycle. MAS also reinforces that cloud adoption must be underpinned by robust governance and risk management practices aligned to the Technology Risk Management (TRM) and outsourcing guidelines, applied proportionately but without dilution.

Importantly, MAS advocates for a pragmatic, risk-based approach to due diligence and ongoing oversight. While FIs may leverage third-party attestations (e.g., SOC 2, ISO 27001, CSA STAR), independent reviews, and market intelligence, they remain ultimately accountable for maintaining continuous monitoring and ensuring ongoing relevance and reliability of external assurances. Industry practices reflect this direction, with firms increasingly complementing certifications with practical validation measures such as pilots, control mapping, and direct engagement.

Overall, the report underscores that accelerating cloud-enabled RegTech adoption will depend on moving beyond siloed approaches toward a more cohesive ecosystem model—one that combines clear accountability, reusable standards, aligned assurance, and strengthened capabilities. This shift is critical not only to improving adoption outcomes, but also to ensuring that innovation is delivered in a manner that is secure, compliant, and aligned with broader regulatory expectations.

#### Key Next Steps- FIs, SIs, CSPs and RegTechs

- **Drive Industry Standardisation & Interoperability:** *Owners: Industry bodies / regulators (facilitator), CSPs, RegTechs, FIs*  
Accelerate development of shared standards such as APIs, data models, and deployment archetypes. Encourage regulator-supported industry utilities and forums to reduce fragmentation and enable scalable, interoperable RegTech ecosystems.
- **Accelerate Adoption via Reusable Artefacts & Trusted Assurance:** *Owners: RegTechs, CSPs, SIs, validated by FIs*  
Package solutions into reusable “adoption kits” (e.g., security packs, deployment blueprints, control mappings, responsibility matrices) complemented by independently verifiable assurance. This reduces FI due diligence burden and shortens time-to-value while maintaining accountability for ethical and compliant outcomes.
- **Clarify accountability and strengthen governance frameworks:** *Joint Owners: FIs, CSPs, RegTechs, SIs*  
Co-develop a federated governance model with clearly defined end-to-end accountability (e.g., RACI matrices aligned to materiality, [see page 15 for further detail](#)) across the delivery lifecycle.

Embed joint risk acceptance aligned to workload criticality, with CSPs and RegTechs providing greater transparency (e.g., shared responsibility models, control boundaries) to enable consistent governance outcomes.

- **Operationalise regulatory requirements through practical frameworks i.e. multi-party accountability chain:** *Joint Owners: FIs, RegTechs, SIs*  
Develop internal playbooks to translate MAS and cross-border regulatory requirements into executable artefacts, including standardised control libraries, data flow maps, and reference architectures. Leverage SIs and RegTechs to co-develop reusable implementation playbooks tailored to different risk tiers.
- **Build Ecosystem-Wide Capability Maturity:** *Joint Owners: FIs, CSPs, SIs*  
Uplift critical capabilities in cloud security, data governance, and AI risk management through coordinated training, embedded tooling, and co-delivery models. CSPs and SIs to provide scalable capability frameworks, while FIs retain accountability for risk ownership and decision-making.
- **Strengthen third-party and concentration risk management:** *Owners: FIs, supported by CSPs, RegTechs*  
Define viable exit, substitution, and recovery strategies for critical services, supported by CSP contingency options and RegTech portability.
- **Standardise Assurance, Testing and Continuous Monitoring:** *Joint Owners: FIs, CSPs, RegTechs, SIs*  
FIs, SIs, CSPs, and RegTechs agree on a common set of testing and assurance requirements for AI and other technology solutions. They should use existing standards, shared testing evidence, and common validation approaches. This can reduce repeated due diligence and make it easier to adopt new solutions.
- **Advance data governance and privacy practices:** *Owners: FIs, CSPs, RegTechs*  
Strengthen data governance through ecosystem-aligned policies on data minimisation, tokenisation, and privacy-enhancing technologies. CSPs and RegTechs to provide transparency on data residency, flows, and processing, enabling FIs to meet jurisdictional compliance obligations.



#### Overarching Theme:

Enable scalable cloud and RegTech adoption through greater standardisation, shared accountability, trusted assurance, stronger governance, and ecosystem-wide collaboration.

## Glossary of Terms

| Term                                                 | Definition                                                                                                                                                                                                                          |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AML (Anti-Money Laundering)                          | Regulatory frameworks and controls aimed at detecting and preventing money laundering activities, often supported by RegTech solutions.                                                                                             |
| API (Application Programming Interface)              | Standardised interfaces enabling systems to communicate and integrate, supporting modular and scalable architectures.                                                                                                               |
| BC / DR (Business Continuity / Disaster Recovery)    | Processes ensuring continuity of operations and recovery of services & systems during disruptions.                                                                                                                                  |
| Cloud Service Provider (CSP)                         | Entity providing cloud infrastructure and services such as compute, storage, and security capabilities.                                                                                                                             |
| CSA STAR (Security, Trust, Assurance & Risk)         | A cloud security assurance program by the Cloud Security Alliance (CSA) that certifies cloud service providers' security controls and practices.                                                                                    |
| Financial Institution (FI)                           | An organisation that provides regulated financial products or services, such as banking, insurance, payments, investment, or capital markets activities, and is subject to regulatory oversight.                                    |
| Identity and Access Management (IAM)                 | Controls governing user identities and access to systems and data in cloud environments.                                                                                                                                            |
| ISO 27001                                            | International standard for information security management systems, used by organisations to establish and certify robust data security controls.                                                                                   |
| KYC (Know Your Customer)                             | Standard due-diligence process in financial services to verify customer identity and assess risk profiles, ensuring compliance with anti-money laundering and other regulatory requirements.                                        |
| MAS (Monetary Authority of Singapore)                | Singapore's financial regulator providing guidance on risk management, outsourcing, and cloud adoption.                                                                                                                             |
| On-Premises (On-Prem)                                | Technology deployment model where systems and infrastructure are hosted and managed within an organisation's own environment rather than in the cloud.                                                                              |
| Personally Identifiable Information (PII)            | Data that can identify an individual, requiring strong protection controls.                                                                                                                                                         |
| PoC (Proof of Concept)                               | A small-scale pilot or prototype implementation used to demonstrate the feasibility and effectiveness of a concept or solution before broader deployment.                                                                           |
| RegTech (Regulatory Technology)                      | Technology solutions that enable automated regulatory compliance, monitoring, and reporting.                                                                                                                                        |
| RACI (Responsible, Accountable, Consulted, Informed) | Framework for defining roles and responsibilities across stakeholders for governance clarity.                                                                                                                                       |
| SOC 2 (System and Organization Controls)             | Independent assurance report verifying that a service provider's internal controls (e.g. security, availability, confidentiality) meet industry-recognised trust criteria.                                                          |
| System Integrator (SI)                               | Entity responsible for implementing and integrating technology solutions within enterprise environments.                                                                                                                            |
| TRM Guidelines                                       | MAS guidelines outlining expectations for managing technology risk, governance, and controls.                                                                                                                                       |
| Workload Criticality                                 | Classification of a workload based on its importance to core operations, customer impact, and regulatory obligations, determining the level of controls and resilience required for cloud deployment.                               |
| SaaS                                                 | SaaS is a cloud-based software delivery model where applications are hosted by a provider and accessed over the internet on a subscription basis.                                                                                   |
| IaaS                                                 | Infrastructure as a Service (IaaS) is a cloud computing model that provides virtualized computing resources over the internet, allowing businesses to rent servers, storage, and networking without the need for physical hardware. |

## Chapter 1: RegTech Evolution & the Cloud Imperative

Across the FI landscape, a clear industry alignment is emerging: cloud is no longer a peripheral technology decision but a foundational pillar underpinning the evolution of RegTech. As institutions face increasing regulatory complexity, data intensiveness, and cost pressures, cloud adoption is being widely recognised as essential for enabling scalable infrastructure, real-time analytics, and operational automation.

This shift reflects a broader consensus that cloud capabilities are intrinsically linked to the next generation of RegTech innovation, particularly in supporting advanced analytics, AI, and emerging agentic AI use cases. The MAS [Project MindForge AI Risk Management Operationalisation Handbook](#) and [HKMA's Supporting Adoption of Artificial Intelligence in Fighting Financial Crime paper](#) offer complementary guidance on operationalising AI governance and supporting the responsible deployment of AI in financial institutions. In this context, cloud is not merely an enabler of efficiency, but a structural prerequisite for firms seeking to embed intelligence, agility, and resilience into their regulatory compliance frameworks. A key prerequisite is therefore a sound understanding of AI regulatory requirements, including broader AI risks such as model risk management, third-party/vendor risk, operational risk, explainability, and accountability across model developers, CSPs, and FIs.

For FIs, the implication is clear: proactive and strategic integration of cloud is becoming a critical determinant of their ability to modernise compliance operations and remain competitive. As such, cloud adoption is increasingly positioned at the centre of enterprise-wide AI and RegTech strategies, shaping not only technology roadmaps but also operating models and risk management approaches. This chapter explores the evolution of RegTech and the cloud imperative, drawing on key insights and observations from FIs, SIs, RegTechs, and CSPs.

### **FIs and SIs**

FIs note a range of interconnected factors shaping their approach to cloud adoption in RegTech, spanning strategic priorities, operational realities, risk considerations, and the growing influence of artificial intelligence. From a strategic perspective, cloud adoption continues to gain momentum, particularly among small and mid-sized institutions driven by the need for scalability, cost efficiency, and faster deployment. At the same time, firms are exploring adopting multi-cloud or hybrid models to mitigate concentration risk and preserve flexibility across providers. However, this progression is tempered by practical constraints as further outlined below.

Many organisations continue to face execution challenges, including limited in-house expertise in cloud and AI, misalignment of skills, and the ongoing influence of legacy systems and prior technology investments on migration decisions. As cloud and agentic AI capabilities scale, there is also a growing recognition that capability-building must extend beyond technical teams to include second- and third-line functions, enabling effective oversight and informed judgement in areas where automation cannot fully substitute human input.

From a risk and supervisory standpoint, cyber and technology risks are increasingly viewed as systemic in nature and often external to direct institutional control. Despite this, such risks are broadly accepted as an inherent part of operating in a digital environment and are not materially slowing adoption. In fact, cloud environments are generally regarded as offering a stronger baseline level of security compared to less mature on-premises infrastructures. Nonetheless, firms continue to place strong emphasis on ensuring supervisory expectations are met, particularly in terms of governance clarity and explainability in complex or outsourced arrangements.

Against this backdrop, the RegTech landscape itself is evolving rapidly along a clear trajectory from manual processes, to automation, and now toward AI-driven decision-making. Agentic AI is emerging as a potential inflection point, with the ability to reshape areas such as client onboarding, control testing, and maker-checker processes. While AI may reduce reliance on certain third parties, it also introduces new considerations around governance, accountability, and model risk management, reinforcing the view that a human-in-the-loop approach remains the most practical near-term model.



At the same time, broader market dynamics are influencing adoption trajectories. RegTech providers are facing increasing cost pressures and industry consolidation, prompting both market exits and accelerated investment in AI capabilities. In this context, the value proposition of cloud-enabled RegTech, particularly in areas such as AML is increasingly framed not only in terms of efficiency or audit outcomes, but also in its contribution to strengthening the integrity of the financial system. These shifts are expected to reshape the vendor landscape, with implications for dependency risk, operational resilience, and long-term sustainability.

SIs continue to play a critical enabling role in this ecosystem, effectively bridging the gap between regulatory expectations and technical implementation. Leveraging cross-client experience, SIs are well positioned to identify repeatable patterns and drive the commercialisation of solutions through pre-configured deployments, playbooks, and standardised integration frameworks, reducing the need for bespoke builds. Their delivery models are also evolving, ranging from rapid, plug-and-play solutions to fully customised implementations. However, several recurring challenges persist in practice. Data readiness is frequently underestimated, particularly the effort required for data engineering and integration. Internal bottlenecks within FIs such as slow procurement processes, security approvals, and resistance from compliance teams can further delay progress. Additionally, many institutions face capability gaps post-implementation, lacking the necessary skills to independently operate and sustain cloud-native solutions once they have been deployed.

### **RegTechs and CSPs (“Providers”)**

Providers broadly reinforced many of the themes observed from FIs, while offering additional perspective on how these dynamics are manifesting from a solution and infrastructure standpoint. Consistent with earlier observations, cloud is increasingly positioned as a foundational enabler of next-generation RegTech, particularly in supporting AI-driven and agentic use cases that require scalable compute power, large-scale data processing, and rapid model iteration. This is driving strong demand for AI-enabled capabilities across core compliance functions such as KYC, transaction monitoring, fraud detection, and advanced analytics, further cementing the intrinsic link between cloud adoption and continued RegTech evolution.

In line with the themes highlighted previously on AI transformation, CSPs noted that AI is effectively redefining the baseline for technology adoption, with many advanced use cases now inherently cloud dependent. However, this shift brings to the forefront a new set of governance challenges that mirror concerns raised by FIs, particularly around explainability, model transparency, and regulatory acceptance of AI-driven decision-making.

The emergence of agentic AI introduces an additional layer of complexity, including novel risks associated with distinguishing between authorised and potentially malicious autonomous agents, in the absence of fully established industry standards or regulatory frameworks. Echoing earlier observations on operational and capability constraints, CSPs emphasised that barriers to adoption are less about the availability of technology and more about gaps in institutional readiness. In particular, gaps in foundational control environments such as identity and access management, logging, network segmentation, and data governance continue to impede effective implementation. These challenges are compounded by shortages in cloud security and AI talent, as well as a heavy reliance on external vendors, which together raise concerns around long-term sustainability and operational resilience, especially for highly customised solutions. As such, there is a shared recognition of the need for broader and more practical upskilling across FIs, extending beyond technical teams to strengthen overall governance and oversight capabilities.

Consistent with the shift described earlier, providers also observed a clear move away from binary deployment decisions toward more nuanced, workload-driven strategies. More mature organisations are increasingly selecting between cloud, on-premises, and hybrid models based on specific use case requirements, data sensitivity, and risk considerations, reflecting a more sophisticated and context-driven approach to technology architecture.

Finally, cost dynamics remain an important, albeit often misunderstood, factor in adoption decisions. Similar to perspectives shared by CSPs, RegTech providers highlighted that cloud value is frequently assessed against sunk investments in legacy infrastructure, leading to incomplete or skewed comparisons. In many cases, the full lifecycle costs of maintaining on-premises environments including ongoing skills requirements, system upgrades, and resilience engineering are underestimated. At the same time, broader cost pressures across the RegTech ecosystem are accelerating the push toward scalable, cloud-based delivery models, reinforcing the longer-term economic and strategic rationale for adoption.

## MAS Insights

### Supervisory Comfort and Scaled Adoption

MAS acknowledges that FIs are increasingly embracing technological innovation to address regulatory and compliance challenges. In this context, MAS has clarified that it continues to support the use of cloud, provided that FIs implement strong governance frameworks and robust risk management practices. Existing regulatory guidelines support this approach by allowing flexibility across private, public, and hybrid cloud deployments.

MAS has observed that adoption of cloud-based RegTech solutions tends to be more advanced in use cases with well-established cloud deployment models and where vendors have undergone multiple rounds of supervisory review. These areas include transaction monitoring, sanctions screening, and regulatory reporting. In addition, there is growing alignment in the digitisation and automation of compliance workflows.

Despite this progress, MAS notes that further opportunities exist to enhance the depth and breadth of cloud-based RegTech implementation. There is scope to improve integration and consistency across end-to-end compliance processes within the ecosystem.

## Key Takeaways

Cloud is now viewed as a strategic necessity, underpinning AI, advanced analytics, and the future of RegTech, rather than a discretionary technology choice. AI adoption, particularly agentic AI is accelerating cloud uptake but introducing new challenges around governance, explainability, and accountability. From the survey conducted with 17 RegTechs, responses indicate ~65% of RegTechs typically adopt a consistent core architecture with limited configurability across clients. This may constrain flexibility to meet institution-specific regulatory nuances, requiring additional customisation layers or process workarounds.

Adoption barriers are therefore exacerbated by FIs needing to configure internal environments to meet RegTech solutions requirements. This is in addition to challenges observed across capability gaps, including skills shortages and difficulty operating core key controls. FIs remain focused on maintaining supervisory comfort, clear accountability, and robust governance despite increasing reliance on cloud environments.

While implementation challenges remain, continued collaboration across regulators and industry participants, coupled with advancing technology and data standardisation efforts, presents a significant opportunity to improve reporting quality, operational efficiency, and overall regulatory compliance outcomes.

## Chapter 2: Cloud Security & Shared Responsibility

As FIs deepen their reliance on cloud to support RegTech and AI-enabled capabilities, attention is increasingly shifting from adoption to accountability, particularly in the context of cloud security and the shared responsibility model. While the industry broadly acknowledges this model as a foundational principle of cloud risk management, its practical application is often uneven, especially as operating models evolve beyond traditional infrastructure-as-a-service (IaaS) into software-as-a-service (SaaS) and AI-driven environments where ownership boundaries become more opaque.

Despite these complexities, there is a clear and consistent understanding across the industry: regulatory accountability ultimately resides with the FI and cannot be outsourced. This principle is becoming more pressing as firms integrate AI and advanced analytics into compliance processes, with associated risks such as data integrity, model governance, and explainability viewed as extensions of existing technology and data risk frameworks rather than entirely new categories.

In this environment, reliance on vendor assurances or certifications alone is increasingly seen as insufficient. Regulators and industry stakeholders expect firms to demonstrate active oversight through robust governance structures, clearly defined roles and responsibilities, and verifiable evidence of control effectiveness. As a result, leading institutions are moving toward more rigorous approaches to third-party risk management, ensuring that cloud adoption is underpinned by disciplined control frameworks that can withstand heightened regulatory scrutiny while enabling innovation at scale.

### **FIs and SIs**

Across both FIs and SIs, a consistent theme is emerging: while the shared responsibility model is well understood in principle, its practical application becomes increasingly complex as cloud and RegTech adoption scale in both scope and materiality.

For FIs, there is a clear demand for more prescriptive and operationally meaningful articulation of “who is responsible for what”, particularly as regulatory-critical workloads migrate to the cloud. Materiality has become the central lens through which responsibility allocation is assessed. For lower-risk, non-material workloads, institutions are generally more willing to rely on CSPs and RegTech vendors to manage technical controls and day-to-day operations. However, as workloads become more material, accountability shifts decisively back to the FI. In conjunction with this, MAS expects governance and control frameworks to be commensurate with the risks involved and sufficiently robust to meet supervisory expectations. **See “MAS Insights” section below for additional details.**

This shift is most evident in areas such as risk acceptance, governance oversight, and ultimate ownership of incident outcomes, reinforcing the principle that regulatory responsibility cannot be outsourced. This dynamic underscores the inherently asymmetric nature of the shared responsibility model. While CSPs and RegTech providers may operate core technical safeguards such as encryption, key management, and infrastructure security the burden of regulatory accountability remains firmly with the FI, regardless of the extent of outsourcing. This asymmetry becomes more pronounced as institutions adopt more complex architectures, including AI-enabled RegTech solutions, where responsibility boundaries are less clearly defined and risks particularly around data usage and model behaviour are amplified.



Data location and sovereignty considerations further complicate this landscape. Although MAS does not impose strict in-country data residency requirements directly, data location continues to materially influence sovereignty risk assessments and supervisory confidence. In practice, FIs highlight a persistent lack of transparency in how critical controls such as identity and access management (IAM), data handling protocols, and incident response processes are implemented and evidenced by providers. The integration of AI use cases compounds these concerns, introducing heightened sensitivity around data leakage, governance clarity, and accountability demarcation. Within this context, the handling of personally identifiable information (PII) has emerged as a critical design and control challenge. There is strong industry alignment on minimising the exposure of raw PII within RegTech platforms wherever possible. Instead, institutions are increasingly adopting techniques such as anonymisation, pseudonymisation, and data abstraction, for example, replacing exact dates of birth with age bands. A guiding principle is taking hold: PII should not be modifiable or “reconstructable” in a manner that enables re-identification, reinforcing a privacy-by-design approach to cloud-based RegTech architectures.

At the same time, regulatory expectations on third-party risk management are creating significant operational tension. MAS “look-through” requirements extend beyond direct vendors to encompass fourth- and even fifth-party dependencies, placing considerable strain on traditional oversight models. In practice, jurisdictional constraints, enforceability of audit rights, and the complexity of back-to-back contractual arrangements often make full compliance challenging at scale. This is particularly evident among smaller institutions, which tend to rely more heavily on vendor certifications and standard disclosures due to limited in-house technical capabilities.

From the SI perspective, many of these challenges crystallise most acutely in the post-implementation phase. While roles and responsibilities may be relatively well defined during initial deployment, ambiguity frequently emerges once solutions move into steady-state operations. Common friction points include ownership of configuration drift as cloud environments evolve, as well as responsibility for periodic re-certification of controls, both of which can lead to unintended degradation of the control environment if not clearly assigned. Further complexity arises regarding monitoring obligations and cost ownership. The scope of logging, alerting, and incident detection responsibilities is often not fully agreed upfront, leading to disputes during operations. In parallel, cloud consumption costs, particularly those associated with data logging and retention, are frequently underestimated during design and become points of contention post go-live.

Finally, the proliferation of tooling across cloud environments introduces additional ambiguity. The overlap between CSP-native capabilities and SI-implemented or third-party solutions often results in unclear delineation of responsibilities, duplication of controls, or gaps in coverage. Without clear ownership and rationalisation, this can undermine both operational efficiency and control effectiveness.

Taken together, these perspectives highlight a fundamental challenge for the industry: translating the shared responsibility model from a conceptual framework into a clearly defined, operationally enforceable construct. As cloud adoption deepens and RegTech solutions become increasingly AI-enabled, achieving this clarity particularly across the full lifecycle from design through to steady-state operations will be critical to ensuring both robust security and sustained regulatory compliance.

### **RegTechs and CSPs (“Providers”)**

From the perspective of Providers, the evolution of cloud-enabled compliance solutions is exposing a different, yet complementary, set of challenges within the shared responsibility model centred on capability gaps, operational realities, and the growing complexity of AI-driven environments. A key observation is that, in practice, the security and compliance responsibilities expected of FIs often exceed their technical capabilities and operating budgets, particularly for smaller firms relying heavily on SaaS-based RegTech solutions. This has led to increasing recognition that the traditional shared responsibility model, originally designed around infrastructure-centric cloud services, may no longer be sufficient. Providers point to the need for an expanded and more explicit articulation of responsibilities across SaaS and AI-driven service layers, ensuring that firms are better informed of the controls, governance measures, and compliance obligations expected of them.

From an operational security standpoint, CSPs emphasise that many institutions would benefit from greater reliance on provider-led capabilities in areas such as continuous monitoring, patch management, security tooling, and infrastructure resilience. These capabilities can often be deployed more consistently and at scale by providers than by individual institutions, which may struggle to maintain equivalent levels of maturity independently. However, this model requires FIs to retain sufficient oversight and assurance mechanisms to demonstrate effective ongoing control, creating a tension between outsourcing execution and retaining accountability.

A recurring theme across both CSPs and RegTech providers is the importance of customer capability, particularly in relation to the implementation of foundational cloud security practices. As FIs accelerate the adoption of AI-enabled RegTech solutions, persistent gaps remain in core areas such as identity isolation, network segmentation, and data governance. These weaknesses are further exacerbated in SaaS environments, where the abstraction of infrastructure can create a false sense of end-to-end vendor responsibility. While providers may support system configuration and baseline controls, customers continue to own critical decisions regarding data policies, retention strategies, and incident outcomes. This challenge is even more pronounced among downstream or non-bank clients, where understanding of shared responsibility constructs is often limited.

Operational inefficiencies also arise from misalignment in lifecycle management practices. CSPs highlight that many FI environments lag in versioning and patch adoption, with customers frequently operating on outdated configurations. In contrast, providers can deploy updates rapidly and at scale, creating a persistent divergence between available and implemented capabilities. This gap not only increases risk exposure but also complicates assurance and support processes.

Education and organisational alignment are identified as additional barriers to effective cloud and AI adoption. Differences in technical understanding across senior management, decision-makers, IT teams, and business users often result in disconnects between those approving investments and those responsible for implementation and operation. This fragmentation can lead to suboptimal design decisions, misinterpretation of risk, and inconsistent control application across the enterprise.

In parallel, providers observe that control frameworks within FIs are not always proportionate or sufficiently tailored to specific use cases. In some instances, institutions adopt overly conservative or duplicative controls, increasing operational complexity and inhibiting innovation without delivering commensurate risk reduction. There is a growing call for more outcome-driven, use-case-specific guidance that distinguishes essential controls from those that create unnecessary overhead.

As AI adoption accelerates, both CSPs and RegTech providers largely view AI-related risks as an extension and amplification of existing technology and data risk frameworks. This includes heightened expectations on governance discipline, clear delineation of roles and responsibilities, robust logging and auditability, and explainability of model-driven outcomes. At the same time, participants acknowledge a set of emerging risks that are more specific to AI deployments, including information leakage, prompt injection vulnerabilities, inconsistent or inadequately enforced guardrails, and challenges in assigning accountability where AI-driven processes result in errors or unintended outcomes.

The emergence of agentic AI further complicates this landscape by blurring traditional accountability boundaries. In scenarios where CSPs host underlying models or infrastructure but do not develop, train, or govern the AI systems themselves, there is often misalignment in expectations. Customers may assume that providers bear responsibility for AI-related risks, while providers position themselves as infrastructure enablers rather than risk owners. This divergence continues to create friction in contractual negotiations, assurance processes, and risk allocation discussions.

In response to these complexities, there is increasing support for the use of controlled testing environments, such as regulatory sandboxes to validate AI-driven RegTech solutions and associated security controls prior to broader deployment. Such environments can enable safer experimentation with emerging technologies, facilitate clearer understanding of risk boundaries, and support the development of more robust governance and control frameworks. Collectively, these perspectives underscore a critical inflection point: as cloud and AI capabilities become more deeply embedded in RegTech ecosystems, the effectiveness of the shared responsibility model will depend not only on clearer delineation of roles, but also on strengthening institutional capability, improving transparency, and aligning expectations across all participants in the value chain.

## Illustrative Common Operating Model for Cloud-Based RegTech Adoption

The successful adoption of cloud-based Regulatory Technology requires a collaborative ecosystem comprising FIs, RegTech providers, cloud service providers, system integrators, and the regulator. Each stakeholder plays a distinct but interconnected role in enabling compliant, secure, and scalable regulatory transformation as outlined below.

|  Stakeholder |  Ecosystem Role |  Key Responsibilities                                                                                                                                                                                                                      |  Strategic Outcomes                                                             |
|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CSPs                                                                                          | Infrastructure Enabler                                                                           | <ul style="list-style-type: none"> <li>Provide secure, scalable, resilient cloud infrastructure, including: <ul style="list-style-type: none"> <li>Cybersecurity</li> <li>Data Protection</li> <li>Operational Resilience</li> <li>Service Availability Capabilities</li> </ul> </li> </ul>                                 | <ul style="list-style-type: none"> <li>Greater scalability</li> <li>Improved resilience</li> <li>Reduced technology overheads.</li> </ul>                          |
| RegTech Providers                                                                             | Capability Enabler                                                                               | <ul style="list-style-type: none"> <li>Deliver solutions aligned with evolving trends and regulatory requirements including (not limited to): <ul style="list-style-type: none"> <li>Compliance, Regulatory Intelligence,</li> <li>Monitoring, Analytics, and Reporting</li> <li>Fraud and Analytics</li> </ul> </li> </ul> | <ul style="list-style-type: none"> <li>Increased automation</li> <li>Improved accuracy</li> <li>Real-time compliance insights</li> </ul>                           |
| FIs                                                                                           | Business & Risk Owner                                                                            | <ul style="list-style-type: none"> <li>Outline and map regulatory requirements</li> <li>Establish governance frameworks</li> <li>Manage data ownership, oversee third-party risks</li> <li>Drive adoption across compliance functions</li> </ul>                                                                            | <ul style="list-style-type: none"> <li>Enhanced compliance effectiveness</li> <li>Reduced operational risk</li> <li>Improved regulatory responsiveness.</li> </ul> |
| SIs                                                                                           | Transformation Orchestrator                                                                      | <ul style="list-style-type: none"> <li>Integrate RegTech solutions with enterprise systems</li> <li>Manage migration and implementation</li> <li>Establish sustainable operating models</li> </ul>                                                                                                                          | <ul style="list-style-type: none"> <li>Accelerated deployment</li> <li>Reduced implementation risk</li> <li>Seamless interoperability</li> </ul>                   |
| Regulators                                                                                    | Ecosystem Steward                                                                                | <ul style="list-style-type: none"> <li>Establish regulatory expectations, technology risk management standards, supervisory guidance, and industry enablement initiatives</li> </ul>                                                                                                                                        | <ul style="list-style-type: none"> <li>Regulatory certainty</li> <li>Responsible innovation</li> <li>Stronger ecosystem with trust and resilience.</li> </ul>      |

### Addressing Common Adoption Challenges

|  Challenge |  Ecosystem Response                                               |
|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Regulatory interpretation and compliance uncertainty                                          | Ongoing engagement between MAS, FIs, and RegTech providers to promote i) consistency and ii) regulatory clarity.                                       |
| Data governance, privacy, and cross-border risks                                              | Clear accountability models supported by controls for e.g. strong cloud controls, data classification standards, and risk-based governance frameworks. |
| Legacy technology integration                                                                 | Use of standardised APIs facilitated by system integrators including modular architecture, and phased implementation.                                  |
| Cybersecurity and operational resilience concerns                                             | Shared responsibility models leveraging cloud-native security controls, continuous monitoring, and resilience testing.                                 |
| Skills and capability gaps                                                                    | Industry-wide capability building through i) training, knowledge-sharing initiatives, and ii) ecosystem partnerships.                                  |

The common operating model should establish a trusted regulatory ecosystem in which FIs retain accountability for compliance outcomes, technology providers deliver specialised capabilities, cloud providers enable resilient infrastructure, system integrators drive implementation, and MAS provides the regulatory guardrails necessary to support responsible innovation.

**Operationalising shared responsibility through a risk-tiered common operating model:** To make the common operating model effective in practice, FIs should translate shared responsibility from a conceptual principle into a lifecycle-based governance framework. This should begin with clear classification of cloud-based RegTech workloads by materiality, criticality, data sensitivity, operational dependency, and AI usage, where relevant. The outcome of this assessment should determine the level of governance, assurance, control validation, and ongoing oversight required across the FI, RegTech provider, CSP, and SI.

This approach should be applied across the full lifecycle, from solution selection and design through to deployment, steady-state operation, incident management, periodic review, and exit planning. For lower-risk workloads, FIs may place greater reliance on provider-managed controls and standard assurance artefacts. For more material or regulatory-critical workloads, FIs should retain stronger oversight through enhanced due diligence, clearer RACI mapping, control testing, evidence review, and senior governance sign-off.

Where AI-enabled RegTech is involved, additional attention should be given to explainability, data usage, model behaviour, guardrails, logging, and accountability for outcomes.

In practical terms, the common operating model should be supported by a defined set of shared responsibility artefacts and operating disciplines, including:

- **Materiality and risk-tiering criteria** that classify workloads based on business criticality, regulatory impact, data sensitivity, operational dependency, and AI risk characteristics.
- **Responsibility mapping** that clearly distinguishes FI-retained obligations from CSP-managed, RegTech-managed, and SI-supported activities across infrastructure, application, data, security, monitoring, and incident response.
- **Control and assurance requirements** that scale according to risk tier, including control mapping, testing evidence, certifications, independent reviews, and ongoing validation of provider controls.
- **Lifecycle governance checkpoints** covering design approval, pre-deployment review, go-live readiness, post-implementation review, periodic reassessment, and exit or substitution planning.
- **AI-specific oversight**, where relevant, covering explainability, data leakage risk, model monitoring, guardrails, auditability, and accountability for automated or AI-assisted outcomes.
- **Continuous monitoring and evidence management** to ensure that shared responsibilities remain effective as cloud configurations, vendor services, regulatory expectations, and FI risk profiles evolve.

## MAS Insights

### Governance Expectation Enablement

MAS emphasises that its supervisory expectations for cloud-based RegTech adoption are anchored in the principles set out in the Technology Risk Management (TRM) Guidelines and the Guidelines on Outsourcing (for FIs other than banks), with a strong focus on governance, accountability, and effective oversight of third-party arrangements, regardless of an institution's size or internal capability. In this context, FIs are expected to adopt governance approaches that reflect clear ownership and robust operationalisation of shared responsibilities across the FI, CSPs, RegTech vendors, and SIs.

MAS underscores that outsourcing does not absolve FIs of their regulatory obligations; accountability remains firmly with the institution, including its board and senior management. Accordingly, FIs should ensure that outsourcing arrangements are structured to adequately identify and manage risks, maintain sufficient control, and support key lifecycle activities such as renegotiation, renewal, or exit. While MAS recognises that operational constraints may vary across institutions, it expects governance and control frameworks to be commensurate with the risks involved and sufficiently robust to meet supervisory expectations.

## Key Takeaways & Next Steps

Security failures are not due to missing tools, but to **misalignment between accountability and capability**, requiring **clearer responsibility models, stronger assurance mechanisms, and improved FI education**.

The four key takeaways and next steps for consideration for industry participants include the following:

### 1 An ecosystem approach is required for adoption:

- Accountability for risk management, oversight, and outcomes is distributed across FIs, SIs, CSPs, and RegTechs, and should be aligned to workload materiality. This reinforces the importance of clearly defined roles, transparent control boundaries, and coordinated risk ownership, irrespective of outsourcing arrangements.
- **Next steps: Clarify internal accountability and materiality thresholds:** Strengthen clarity on responsibility and materiality thresholds through a collaborative approach across FIs, SIs, CSPs, and RegTechs, supported by standardised responsibility mapping and clearer articulation of risk ownership across cloud and AI use cases. This can be further enabled by shared frameworks and guidance to ensure consistent application across different deployment models.

### 2 Shared responsibility requires clearer definition:

- Greater clarity is needed, particularly for SaaS and AI, where roles around data, controls, and AI risk ownership remain ambiguous.
- **Next steps: Strengthen shared responsibility articulation with providers:** FIs, SIs, CSPs, and RegTechs should jointly define clearer operating boundaries, particularly for SaaS and AI, covering data handling, IAM, incident response, AI governance, and the distinction between CSP-managed, RegTech-managed, and FI-retained controls.
- **Additional consideration:** To reduce ambiguity and adoption friction, CSPs could look to provide additional transparency over reference architecture, control design, and data handling boundaries, supported by reusable implementation artefacts that clearly distinguish provider-managed controls from FI-owned obligations.

### 3 Capability and control gaps persist:

- There is scope to increase awareness of cloud security fundamentals, patching, and stakeholder understanding, which continue to challenge effective risk management.
- **Next steps: Enhance cloud security baseline capabilities:** Advance core cloud security practices through a shared capability uplift across the ecosystem, spanning areas such as identity management, network security, data governance, and patching. This should be enabled by greater collaboration between FIs, SIs, CSPs, and RegTechs, with CSPs and RegTechs providing clearer implementation guidance and tooling to help align platform, application, and customer-managed controls in a more integrated and accessible manner.

### 4 Data, third-party, and AI risks are intensifying:

- Data governance, auditability across supply chains, and AI-related risks are increasing complexity and supervisory expectations.
- **Next Step 1: Reinforce data governance and third-party risk management:** Undertake joint efforts across CSPs, SIs, FIs, and RegTechs to strengthen controls over PII (e.g. anonymisation), improve transparency over data flows and locations, and apply risk-based oversight of downstream providers.
- **Next Step 2: Establish robust AI risk management and testing practices:** FIs, SIs, CSPs, and RegTechs should implement a collective approach to AI governance, including explainability, logging, and guardrails; clarify accountability in agentic AI scenarios; and leverage controlled environments (e.g. sandboxes) for testing prior to deployment. These recommendations are consistent with MAS-led initiatives, including the [AI Risk Management Toolkit and FEAT principles](#) and most recent guidance for [Safeguard for Agentic Finance at Runtime \(SAFR\)](#), which provide practical guidance on AI governance, accountability, transparency, risk management, and responsible AI adoption.

## Chapter 3: Data Sovereignty, Privacy & Regulatory Compliance

As cloud adoption accelerates across FIs, data sovereignty and privacy considerations are emerging as critical determinants of both regulatory acceptance and operational design. While there is broad industry support for outcome-based regulation, allowing flexibility in how firms meet supervisory expectations, institutions continue to face practical challenges in translating high-level regulatory principles into implementable, auditable controls within cloud environments.

At the centre of this tension lies the handling of sensitive and personal data. Data sovereignty, cross-border data flows, and the use of PII remain persistent friction points, often shaping architectural decisions and cloud deployment strategies. In response, firms are increasingly prioritising data minimisation, anonymisation, and abstraction techniques as core design principles, reducing reliance on the movement or exposure of raw PII within RegTech solutions.

However, there is also growing recognition that data protection considerations must be assessed in context. Rather than defaulting to risk-averse or exclusionary approaches, leading institutions are adopting more nuanced, use-case-driven evaluations considering the specific regulatory requirements, system architecture, risk profile, and jurisdictional factors involved. This shift reflects a maturing industry perspective: one that balances the need for robust data protection with the strategic imperative to leverage cloud capabilities in a compliant and scalable manner.

### **FIs and SIs**

Across both FIs and SIs, data sovereignty and privacy are key pressure points in cloud adoption, with a shared focus on maintaining regulatory confidence while enabling scalable, cloud-based RegTech solutions. For FIs, the priority centres on sustaining defensible regulatory positions and achieving supervisory comfort, particularly in areas where regulatory requirements remain open to interpretation. Data residency, access controls, and jurisdictional oversight continue to drive architectural decisions, with cross-border data flows presenting ongoing complexity due to differing regulatory expectations. Institutions are increasingly adopting a cautious posture toward sensitive data, retaining PII internally and limiting external exposure through tokenisation, anonymisation, and abstraction techniques to reduce re-identification risk.

A persistent challenge lies in interpretive uncertainty, especially for mid-tier firms with more limited internal resources. This has led to greater reliance on external legal guidance and iterative reassessment as supervisory expectations evolve. At the same time, firms emphasised the importance of clearly evidencing risk-based approaches to regulators, particularly to address perceptions that cloud environments are less transparent than on-premises systems. This is further complicated by the need to balance AI-driven innovation with stringent data minimisation and privacy requirements. To address these challenges, FIs are seeking more practical, implementation-focused support, including reference architectures, worked examples of proportionate cloud deployments, clearer identification of mission-critical workloads, and flexibility to adopt hybrid or partially on-premises models.

From the SI perspective, many of these issues manifest as execution and design constraints. Cross-border data restrictions and localisation requirements can be difficult to reconcile with globally standardised cloud architectures, particularly for AI-enabled or managed services. Late-stage regulatory clarification often necessitates costly re-architecture, reinforcing the need for earlier and more prescriptive guidance. As a result, SIs are calling for greater standardisation and clarity, including regulatory-to-technical control mappings, reusable compliance templates, and reference deployment models.

Overall, both groups are highlighting the need for clearer, more actionable guidance that bridges regulatory intent and technical implementation, enabling firms to manage sovereignty and privacy risks confidently without constraining the strategic benefits of cloud adoption.

### **RegTechs/CSPs (“Providers”)**

From the RegTech and CSP perspective, data sovereignty and privacy requirements are less a question of principle and more a challenge of practical feasibility, cost, and consistency of implementation, particularly for smaller or non-bank FIs. A key concern is the complexity of operationalising sovereignty and privacy controls. Even where firms have established legal and privacy frameworks, translating requirements into enforceable technical controls—such as managing cross-border data flows, residency constraints, and retention or deletion rules—remains difficult in practice. This is often compounded by inconsistent interpretation of regulatory expectations across FIs, resulting in bespoke implementations that increase both delivery complexity and ongoing assurance overhead.

Providers also emphasise that data sovereignty risks should be assessed contextually, rather than treating cloud environments as inherently higher risk. Effective risk management depends on a combination of factors including use cases, data classification, architecture, jurisdiction, and control design, rather than the deployment model alone.

However, in practice, heightened sensitivity around PII continues to constrain adoption, particularly for data-intensive analytics and AI use cases, unless supported by robust privacy-enhancing techniques such as tokenisation or encryption.

At the same time, providers highlight a persistent gap between technical capability and institutional adoption. A wide range of mechanisms such as regional deployment models, distributed architectures, and advanced encryption already exist to address sovereignty and privacy concerns. However, these are often underutilised due to limited understanding, confidence, or regulatory clarity among FIs and stakeholders. Importantly, the availability of tooling, including policy-as-code and CSP-native controls, does not remove the need for firms to define risk appetite, governance frameworks, and control strategies.

To address these challenges, RegTechs and CSPs are calling for more standardised, practical, and tiered implementation guidance. This includes reusable artefacts (e.g. data flow mapping templates), clearer regulatory-to-technical control mappings, and common benchmarks or checklists to reduce interpretive divergence. Adoption is notably more effective where providers embed “transparency by design”, offering clear visibility into data residency, processing methods, encryption and retention practices, enabling FIs to more easily demonstrate compliance.

Finally, providers note that even where technical risks are well managed, reputational considerations continue to drive cautious adoption, particularly in cross-border scenarios. As a result, improved documentation, greater transparency, and increased supervisory clarity are seen as critical enablers in bridging the gap between regulatory intent and scalable cloud implementation.



## Key Takeaways and Next Steps

The primary gap is not regulatory intent, but the ability to **translate principles into practical, defensible operating models**, particularly for AI-driven use cases.

The four key takeaways and next steps for consideration for industry participants include the following:

### 1 Outcome-based regulation is valued, but standardizing implementation remains a challenge.

- Outcome-based regulation is widely supported, but firms often struggle to translate high-level regulatory principles into practical and auditable controls. As a result, different interpretations across the industry can lead to inconsistent implementation approaches and outcomes.
- **Next step 1:** Develop industry-standard playbooks, control frameworks, checklists, and reusable artefacts that convert regulatory principles into actionable guidance.
- **Next Step 2:** Increase collaboration between FIs, SIs, CSPs, RegTechs, industry bodies, and regulators to promote consistency, reduce duplication, and accelerate adoption of leading practices.
- Translate regulatory principles into actionable controls through collaborative playbooks co-developed by FIs, SIs, CSPs, RegTechs, and industry bodies, supported by practical examples and use-case-driven guidance.

## 2 Data sovereignty and PII handling are key friction points:

- Data residency and cross-border rules drive cautious adoption. FIs prefer anonymisation and tokenisation over sharing raw PII.
- **Next steps:** Strengthen data classification, minimisation, and adoption of privacy-enhancing technologies through joint enablement across FIs, SIs, CSPs, and RegTechs, supported by clearer regulatory engagement on cross-border data expectations.

## 3 Accountability and risk assessment must be clear and contextual:

- FIs focus on maintaining supervisory comfort and clear accountability. Risk assessments are increasingly tailored to use case, data, and jurisdiction.
- **Next steps:** Improve transparency of accountability structures and risk assessments through aligned articulation of shared responsibilities, with industry and regulators providing clearer guidance on acceptable risk-based approaches.

## Chapter 4: Risk Management, Governance & Operational Resilience

As FIs scale their use of cloud-based RegTech solutions, the focus is shifting toward how cloud adoption is governed, controlled, and sustained from a risk and resilience perspective. While cloud can materially enhance operational resilience, this outcome is not automatic; it depends on deliberate architectural design, including redundancy, failover capabilities, and robust operational controls.

In practice, achieving this resilience is complicated by persistent ambiguity in roles and responsibilities across the ecosystem. Accountability is often fragmented between FIs, CSPs, SIs, and RegTechs, particularly during implementation and transition to steady-state operations.

At the same time, concentration risk within cloud ecosystems is increasingly recognised as a structural constraint rather than a fully mitigable issue. As a result, institutions are expected to manage this risk proactively through strengthened governance, diversification strategies, and enhanced oversight frameworks, ensuring resilience is built into both technology design and operating models.

### **FIs**

FIs emphasise that, while the shared responsibility model provides a useful conceptual foundation for cloud risk management, its practical application remains inconsistent. In all cases, FIs retain ultimate accountability for governance, risk outcomes, and incident response, even where execution is outsourced to CSPs, SIs, or RegTechs.

This accountability is compounded by structural and commercial constraints. Smaller or mid-tier FIs often have limited ability to influence CSP operating models or enforce accountability beyond contractual terms, particularly given the standardised nature of hyperscale cloud services. Any rebalancing of responsibilities typically carries implications for pricing, liability, and innovation, requiring careful trade-offs. In response, MAS has emphasised that its expectations for due diligence in cloud-based RegTech adoption are guided by a risk-based and proportionate approach that FIs will need to factor in. Additionally, to address some of the capability constraints impacting smaller FIs, MAS considers it appropriate for FIs to leverage complementary assurance mechanisms such as independent reviews, audit reports, certifications, and broader market feedback to supplement internal due diligence efforts. **See “MAS Insights” section below for additional details.**

In response, there is strong support for a more explicit and operationally aligned delineation of roles across the ecosystem. FIs increasingly view responsibilities as distributed but distinct: CSPs are typically expected to lead on platform security and infrastructure resilience; RegTech providers on application integrity and secure service delivery; and FIs on governance, oversight, and regulatory outcomes.

Finally, the principles-based regulatory approach introduces a level of subjectivity that places greater emphasis and dependency on ecosystem alignment. Institutions must clearly define their positions in relation to their business model, risk appetite, and control environment, while ensuring consistent understanding across stakeholders. This makes strong governance, clear accountability frameworks, and well-evidenced decision-making critical to sustaining both regulatory confidence and operational resilience.



### **RegTechs and CSPs (“Providers”)**

From the perspective of Providers, the primary challenge lies in driving consistency, efficiency, and transparency across an increasingly fragmented delivery and assurance landscape.

A key friction point highlighted is the duplication of vendor assurance processes. Despite the availability of established certifications (e.g. SOC, ISO), these are not consistently leveraged by FIs, resulting in repeated, bespoke due diligence requests that increase cost and operational burden without delivering materially better risk insight.

Providers highlight the need for standardised assurance baselines, stronger control mappings, and reusable documentation to streamline this process.

Standardised deliverables such as reference architectures, deployment blueprints, responsibility matrices, data lineage views, and evidence inventories can significantly reduce due diligence friction and support more efficient, risk-based assessments.

At the same time, role clarity remains inconsistent across implementations, particularly at the interfaces between CSPs, RegTechs, SIs, and FIs. Providers emphasise the need for more standardised and contractually defined responsibility models, supported by clear RACI frameworks spanning infrastructure, platforms, data flows, and AI components.

Supporting this, transparency and documentation are viewed as essential to effective supervisory engagement. Enhanced reporting, clearer architectural visibility, and well-structured assurance artefacts enable FIs to more confidently demonstrate compliance and explain their cloud arrangements to regulators. However, inconsistent expectations around testing and assurance continue to create uncertainty. There is no common benchmark for what constitutes “sufficient testing,” particularly for AI-enabled solutions, where expectations around stress testing, accountability, and incident response are still evolving. Controlled testing environments, such as sandboxes, are seen as a practical way to address this gap.

While certifications remain important, providers stress that these must be complemented by decision-useful artefacts, including control-to-regulation mappings, scope definitions, testing coverage, and evidence of operating effectiveness tailored to the specific service being adopted. Finally, providers highlight that structural risks, particularly concentration risk, require active governance rather than assumed mitigation. Given the concentration of the CSP market, resilience depends on robust dependency mapping, business continuity planning, and credible exit strategies. At the same time, greater visibility into downstream third-party dependencies is critical to enable effective risk management and regulatory oversight.

Overall, RegTechs and CSPs emphasise the need for standardisation, transparency, and clearer alignment of expectations to reduce complexity, strengthen assurance, and support scalable cloud adoption.

## MAS Insights

### Third-Party and Nth-Party Visibility

MAS underscores that its expectations around third-party and nth-party visibility in cloud-based RegTech arrangements are grounded in the principle that FIs must maintain full oversight and control, even where service delivery involves multiple layers of providers, such as cloud service providers, AI model vendors, and data providers. Adopting a risk-based approach to outsourcing, MAS expects the depth of due diligence and ongoing assessment to be proportionate to the criticality and materiality of the arrangement. In practice, this means FIs should establish governance and monitoring frameworks that provide sufficient transparency across downstream dependencies, ensuring risks are effectively identified and managed throughout the service chain. Importantly, MAS expects FIs to exercise oversight over outsourced services as if they were performed in-house, with accountability remaining firmly with the institution regardless of the complexity of the provider ecosystem.

### Due Diligence Capability Constraints

MAS emphasises that its expectations for due diligence in cloud-based RegTech adoption are guided by a risk-based and proportionate approach, where the depth and frequency of assessment should align with the criticality of the service arrangement. Higher-risk or business-critical services are expected to undergo more rigorous and ongoing evaluation. At the same time, MAS recognises that FIs may face practical constraints in conducting detailed technical assessments of complex or widely adopted third-party solutions, including those provided by cloud service providers and RegTech vendors. In such situations, MAS considers it appropriate for FIs to leverage complementary assurance mechanisms such as independent reviews, audit reports, certifications, and broader market feedback to supplement internal due diligence efforts. Notwithstanding these alternative approaches, MAS underscores the importance of continuous monitoring, with FIs expected to regularly review external assurance outputs and other relevant information to ensure that risks remain effectively managed throughout the lifecycle of the outsourcing arrangement.

## Key Takeaways and Next Steps

Cloud can enhance operational resilience, but only where it is intentionally designed through robust architecture and controls. However, roles and responsibilities across FIs, SIs, CSPs, and RegTech providers remain inconsistently defined, despite FIs retaining full accountability for risk and compliance outcomes. Concentration risk is recognised as structural, requiring active governance through oversight, exit planning, and dependency management rather than reliance on diversification alone.

FIs face challenges in meeting supervisory expectations, particularly around accountability, exit strategies, and defining “sufficient testing” within a principles-based regulatory framework. At the same time, inefficiencies in vendor assurance, lack of standardised testing expectations, and limited visibility over downstream dependencies highlight the need for greater standardisation, transparency, and coordination across the ecosystem.

The three key takeaways and next steps for consideration for industry participants include the following:

### 1 **Role across the ecosystem requires greater clarity and specificity:**

- Responsibilities across FIs, SIs, CSPs, RegTechs, and other parties are inconsistently defined in practice. There is strong demand for more prescriptive, standardised responsibility frameworks.
- **Next step 1:** Develop and adopt standardised RACI models across cloud and RegTech stacks, supported by clear contractual definitions of roles, responsibilities, and liabilities.
- **Next step 2:** Strengthen accountability through clear, shared ownership of risk and controls across FIs, SIs, CSPs, and RegTechs, including in outsourced models.

### 2 **Assurance and testing approaches are fragmented and inefficient:**

- Duplicative due diligence and inconsistent expectations for “sufficient testing” create inefficiencies and uncertainty. Greater standardisation and reliance on existing certifications are needed.
- **Next steps:** Align on standardised assurance baselines (e.g. leveraging SOC/ISO) and define minimum testing requirements, including for AI use cases.

### 3 **Third-party and concentration risks require stronger governance and visibility:**

- Structural concentration risk and complex dependency chains (including nth parties) necessitate enhanced oversight, clearer exit strategies, and improved transparency to support effective risk management.
- **Next steps:** Strengthen third-party risk frameworks through dependency mapping, clear exit strategies, and improved visibility of nth-party arrangements.

## Chapter 5: Strategic Value & Business Case for Cloud-Based RegTech

The strategic rationale for cloud-based RegTech adoption has evolved significantly. Cost efficiency, once a primary driver, is no longer sufficient on its own. Instead, firms are increasingly framing the business case around scalability, resilience, agility, and long-term sustainability, alongside the need to meet growing regulatory expectations.

Cloud is now viewed as a strategic enabler of regulatory transformation, supporting faster adaptation to regulatory change, improved interoperability across systems, and more scalable operating models. Equally important is its role in strengthening regulatory credibility and stakeholder trust, through enhanced transparency, control, and responsiveness.

Reflecting this shift, institutions are moving away from a binary “cloud versus on-premises” mindset toward a more nuanced, workload-driven approach, selecting deployment models based on specific use cases, risk profiles, and regulatory considerations.

Publicly reported case examples indicate that cloud- and AI-enabled RegTech solutions can deliver approximately 60–80% reductions in false positives or alert handling effort, approximately 60% reductions in manual reporting workload, and up to 3× faster audit response times, alongside faster deployment timelines and material operational savings. Cloud-based compliance solutions can significantly compress deployment timelines, with case examples showing approximately 85% faster release cycles (from weeks to days) and rapid MVP deployment within days, compared with longer on-premises implementation cycles.

At the same time, cloud provides access to advanced capabilities, particularly in AI and data analytics, which are increasingly critical to modern RegTech, yet often costly or impractical for institutions to develop and sustain independently. Together, these factors position cloud not simply as an infrastructure choice, but as a cornerstone of future-ready, digitally enabled compliance strategies.



### **Fls**

Fls indicate that the business case for cloud-based RegTech is still maturing, shaped by both evolving strategic priorities and ongoing challenges in demonstrating realised value. A recurring issue is the difficulty of translating broader benefits into measurable outcomes, with gains such as agility, scalability, and enhanced data capabilities often harder to quantify than traditional compliance or cost metrics.

Nonetheless, cloud is increasingly viewed as a practical enabler of capability uplift, supporting faster implementation, elastic scaling, and access to external expertise that would be difficult to replicate in-house. For many firms, particularly those with constrained resources, this represents a meaningful shift in operating model. However, value realisation remains uneven, constrained by interoperability gaps, integration complexity, and continued sensitivities around data control and security, which can dilute anticipated efficiency gains.

Consequently, firms are reframing their business cases toward longer-term strategic outcomes, including improved coordination across jurisdictions, greater responsiveness to regulatory change, and enhanced resilience and testing capabilities. Cloud adoption decisions are therefore increasingly anchored in enterprise-wide considerations, balancing flexibility and innovation with the need to manage geopolitical exposure, data sovereignty risks, and vendor concentration.

Within this context, the growing role of AI-enabled RegTech is further reinforcing cloud's strategic importance, positioning it not only as an infrastructure decision, but as a key enabler of future scalability and the ability to operate effectively across complex, multi-regulatory environments.

### **RegTechs and CSPs (“Providers”)**

From the perspective of Providers, the articulation of a compelling business case for cloud adoption remains closely aligned with the challenges identified by FIs, particularly in demonstrating measurable value beyond compliance. Providers highlighted that it remains difficult to clearly quantify impact in a way that resonates across institutions with differing priorities and levels of maturity. As with the FI perspective, there is a clear shift away from cost-centric narratives toward a broader definition of value, encompassing trust, interoperability, and operational agility. In this context, cloud-based RegTech is increasingly positioned as a strategic enabler of capability uplift, supporting scalability, resilience, AI and machine learning capabilities, cross-border monitoring, and the modernisation of legacy compliance infrastructures.

Consistent with earlier observations on capability constraints and adoption barriers, providers emphasised that trust, education, and more tailored value propositions are critical to scaling adoption. While jurisdictions such as Singapore are seen as trusted hubs for cross-border data processing, this is contingent on robust governance and control frameworks. However, adoption is often slowed by a continued focus on cost-based decision-making and the absence of differentiated, maturity-driven value narratives. As such, vendors play an important role in bridging this gap by more clearly articulating use cases, safeguards, and long-term benefits in a manner that aligns with institutional needs.

At a broader ecosystem level, the ability to scale value is further constrained by the lack of standardisation, echoing earlier themes around fragmentation and interoperability challenges. The absence of consistent metrics to assess outcomes such as efficiency gains, audit readiness, or risk reduction limits comparability and slows adoption. Greater collaboration across the industry, including the development of shared artefacts, common standards, interoperable architectures and standardised APIs, is seen as critical to enabling more repeatable and scalable implementation. In this regard, providers noted that adoption can be significantly accelerated where trust artefacts are effectively productised for example, through pre-defined deployment blueprints, baseline control frameworks, and transparent architecture and data handling documentation, thereby streamlining procurement and due diligence processes while enhancing stakeholder confidence.

Finally, providers also pointed to emerging areas of strategic value that extend beyond traditional compliance objectives. Cloud-enabled capabilities are increasingly supporting cross-border fraud detection and intelligence sharing, leveraging regional and multi-cloud architectures to deliver advanced analytics while addressing data residency and sovereignty considerations. This reinforces the broader narrative consistent with FI perspectives that the value of cloud in RegTech is evolving toward enabling system-wide resilience, connectivity, and insight, rather than simply delivering incremental efficiency gains.

## **Key Takeaways**

FIs continue to see cloud adoption as a strategic enabler, delivering benefits such as scalability, operational efficiency, access to specialised expertise, and greater flexibility in responding to evolving business and regulatory requirements. While organisations recognise these benefits, quantifying value beyond compliance and risk reduction remains an area of ongoing focus. The business case for cloud is increasingly extending beyond cost considerations, with growing emphasis on regulatory agility, cross-border connectivity, and advanced capabilities such as AI and analytics.

RegTechs and CSPs similarly observe that defining and communicating measurable value can vary across FIs due to differing levels of maturity, operating models, and adoption priorities. As a result, strategic value is increasingly associated with factors such as trust, interoperability, operational resilience, and agility.

Adoption is further shaped by the need for stronger ecosystem collaboration, clearer metrics, and tailored value propositions, while cloud-enabled capabilities such as cross-border fraud detection and data insights are emerging as key long-term value drivers.

## Conclusion

The findings of this report highlight a financial services sector that has moved beyond the question of whether cloud adoption should occur and is now focused on how it can be implemented at scale while maintaining resilience, governance, and regulatory trust. Cloud technology is increasingly viewed not simply as a platform for infrastructure modernisation, but as a strategic enabler of innovation, operational agility, advanced analytics, AI adoption, and enhanced customer outcomes.

Across financial institutions, system integrators, cloud service providers, and RegTech firms, there is broad alignment on the opportunities presented by cloud technologies. At the same time, stakeholders recognise that the pace and scale of adoption will depend on the industry's ability to address complex challenges relating to data sovereignty, privacy, operational resilience, third-party risk, and the governance of emerging technologies such as AI.

The discussions undertaken as part of this report suggest that the next phase of cloud maturity will be defined less by technological capability and more by the effectiveness of collaboration across the ecosystem. Financial institutions, technology providers, and regulators each play a critical role in translating regulatory intent into practical implementation, strengthening trust in cloud-based operating models, and supporting the development of consistent industry practices. Continued engagement between these stakeholders will be essential to address common challenges, reduce implementation uncertainty, and accelerate responsible innovation.

Looking ahead, several themes are expected to shape the future landscape. These include greater adoption of AI-enabled solutions, increased use of cloud-native architectures, enhanced automation of compliance and risk management processes, and stronger industry-wide approaches to data governance and operational resilience. As technologies continue to evolve, governance frameworks, accountability mechanisms, and risk management practices will need to evolve alongside them.

Ultimately, organisations that successfully balance innovation with robust governance will be best positioned to realise the full strategic benefits of cloud adoption. By fostering collaboration, strengthening risk management capabilities, and embracing practical, risk-based approaches to technology governance, the financial services industry can continue to unlock new opportunities while maintaining the safety, stability, and trust that underpin the sector.

### Looking Ahead



The future of cloud adoption in financial services will be driven by ecosystem collaboration, responsible innovation, and strong governance that enables organisations to scale cloud and AI capabilities while maintaining trust, resilience, and regulatory compliance.

### **About SFA**

The SFA is a cross-industry non-profit organisation. Its purpose is to support the development of the FinTech industry in Singapore and facilitate collaboration among participants and stakeholders. The SFA is a member-based organisation with more than 600 members. It represents the full range of stakeholders in the FinTech industry, from early-stage innovative companies to large financial players and service providers.

To further its purpose, the SFA also partners with institutions and associations in Singapore and globally to cooperate on initiatives relating to the FinTech industry. Well-connected globally, the SFA has signed more than 70 international Memoranda of Understanding (MoUs) to build its network for members and the broader ecosystem.

For more information, visit <https://singaporefintech.org/>



### **About KPMG**

KPMG in Singapore is part of a global organization of independent professional services firms providing Audit, Tax and Advisory services. KPMG operates in 143 countries and territories with more than 273,000 partners and employees working in member firms around the world. Each KPMG firm is a legally distinct and separate entity and describes itself as such. KPMG International Limited is a private English company limited by guarantee. KPMG International Limited and its related entities do not provide services to clients.

### **DISCLAIMER**

**This report was sponsored by Singapore Fintech Association (“SFA”). Nothing in this report constitutes or implies any endorsement, recommendation or favouring by SFA of KPMG, its services, or any views, products or services referred to in this report. The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although SFA and KPMG endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. To the fullest extent permitted by applicable law, SFA, KPMG Services Pte. Ltd. and KPMG International Limited accept no responsibility or liability whatsoever whether arising in contract, tort (including negligence), breach of statutory duty or otherwise, for any loss, damage, cost or expense arising directly or indirectly from, or in connection with, any person’s use of, reliance on, or inability to use or rely on, this report or any information contained in it.**

**© 2026 KPMG Services Pte. Ltd. (Registration No: 200003956G), a Singapore incorporated company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee.**

**All rights reserved.**

**The KPMG name and logo are registered trademarks or trademarks of KPMG International.**