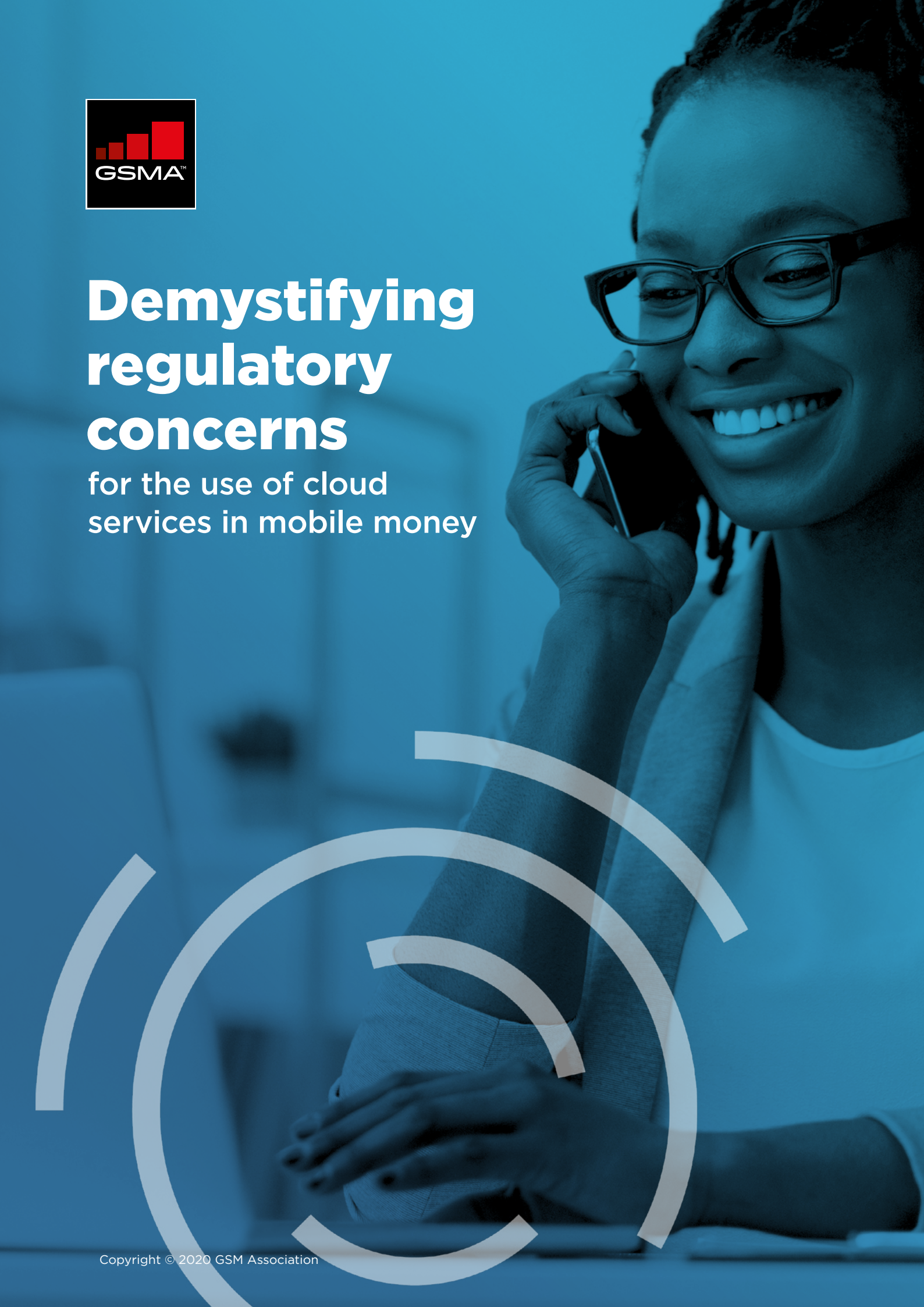


Demystifying regulatory concerns

for the use of cloud services in mobile money

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in **Barcelona**, **Los Angeles** and **Shanghai**, as well as the **Mobile 360 Series** of regional conferences.

For more information, please visit the GSMA corporate website at **www.gsma.com**.

Follow the GSMA on Twitter: **@GSMA**

Mobile Money

The GSMA's Mobile Money programme works to accelerate the development of the mobile money ecosystem for the underserved.

For more information, please contact us:

Web: **www.gsma.com/mobilemoney**
Twitter: **@GSMAMobileMoney**
Email: **mobilemoney@gsma.com**

Lead author:
Juliet Maina, Advocacy and Regulatory Manager, Mobile Money

The GSMA Mobile Money team would like to thank Vodacom for their time and guidance on the development of this report. This report was written with key insights and feedback from Mariana Lopez, Killian Clifford and Jade Nester.

THE MOBILE MONEY PROGRAMME IS SUPPORTED BY THE BILL & MELINDA GATES FOUNDATION AND FLOURISH VENTURES.

Published March 2020

Contents

1.	Introduction	4
2.	What is cloud computing?	6
3.	Benefits of the cloud for mobile money	7
4.	Digital banking on the cloud: Case studies	10
5.	Regulatory concerns	12
6.	Implications of data localisation requirements	14
7.	Overview of global practices by financial regulators	16
8.	The role of financial regulators	18
9.	The role of mobile money providers	20
10.	Conclusion	23
Appendix 1: The demystification of regulatory concerns around the use of cloud		24
Glossary		26

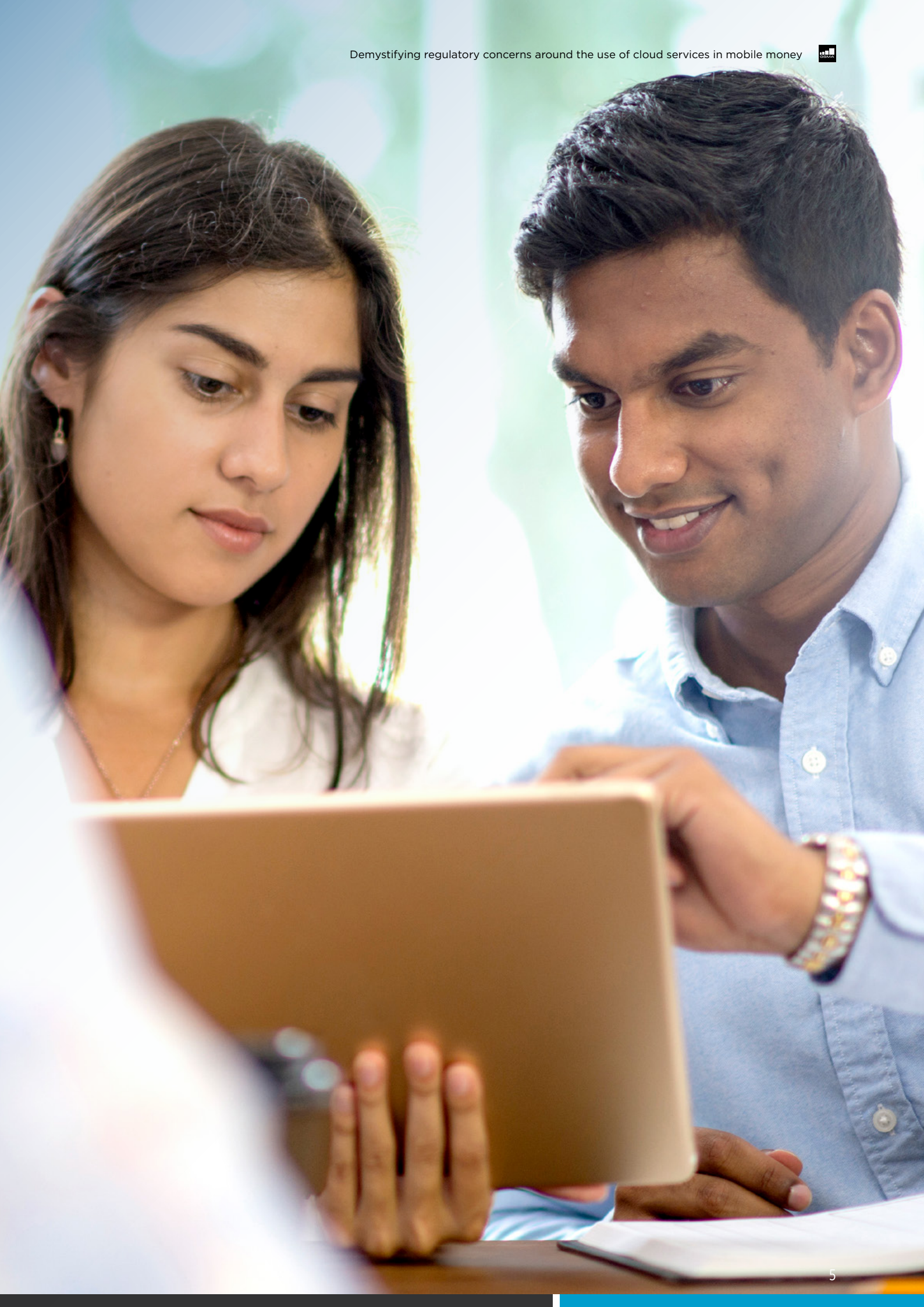
1. Introduction

Cloud services offer a number of benefits to organisations such as economies of scale, flexibility, operational efficiencies and cost-effectiveness.[1] Globally, players in the financial services industry are now adapting their business models to embrace the cloud, and leverage new solutions provided by financial technology providers (fintechs) in order to improve their services and lower their investment costs.[2] For the mobile money industry, there is need to adopt these technological changes to increase scalability and contribute to bridging the financial inclusion gap in a sustainable manner.

While promising several benefits, the cloud can also introduce risks that need to be understood, identified and mitigated. Currently, there are several misperceptions around the effective and secure use of the cloud which, while relevant, are based on traditional banking regulatory concerns. In some markets, this has led to a prohibitive approach towards cloud computing, which is causing uncertainty among mobile money providers about how to adopt the cloud while adhering to existing legal and regulatory frameworks. This uncertainty ultimately acts as a barrier to using the cloud in a way that will be beneficial to the mobile money industry and its continued efforts towards bridging the financial inclusion gap.

Consequently, the objective of this report is to demystify the regulatory concerns regarding the use of cloud computing in the mobile money industry and to explain how restrictions associated with these concerns can be addressed without prohibiting the use of the cloud. It also explains why failure to do so can prevent mobile money providers (MMPs) from realising the benefits of this technology to ensure the continued and inclusive growth of mobile money services. Additionally, this can prevent other players in the ecosystem from leveraging the cloud for innovation and scalability which can be beneficial for the entire mobile money industry, and especially the end user. The report concludes by making practical recommendations for regulators and MMPs to mitigate the risks associated with the adoption of cloud and cross-border movement of personal data which are based on international best practices. It is key for the success of the industry that MMPs and regulatory authorities collaborate to continually foster responsible innovation and drive financial inclusion.

1. Deloitte (2017). EBA guidance on the Cloud. What to consider from regulatory (outsourcing) and security (cyber) point of view.
2. European Banking Authority (2019). Final Report on EBA Guidelines on outsourcing arrangements.



2. What is cloud computing?

Cloud computing is constantly evolving and therefore can be difficult to define. Broadly, the term 'cloud computing services' refers to on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, software, applications, storage equipment, and services).[3] Essentially, the cloud is defined by its characteristics and capabilities; the type of service models describes on how these can be utilised by the user. These are Software as a service (Saas), Platform as a service (Paas) and Infrastructure as a service (Iaas). The key differences between these service models are highlighted in Table 1.

Cloud services can be further defined by the deployment model. In addition to selecting a service model, users and organisations can also determine what kind of deployment model is most suitable for their use. The model defines the level of control the user has versus the cloud service provider (CSP), i.e. who owns the infrastructure (including physical infrastructure such as computers, networks, and storage equipment); who is responsible for the operation of the service; where the infrastructure is located; and who can access it.[4] There are four deployment models; the private cloud, community cloud, public cloud, and hybrid cloud.

Table 1

Service models for cloud delivery

Software as a Service (SAAS)	Platform as a Service (PAAS)	Infrastructure as a Service (IAAS)
The user receives a complete service and does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, and storage.	The user receives a platform and can develop applications and possibly configuration settings for the application-hosting environment.	The user receives fundamental computing resources and can deploy and run arbitrary software, including operating systems and applications.
Examples: **Microsoft O365, G Suite, Gmail, Salesforce**	Examples: **Amazon Web Services, Microsoft Azure**	Examples: **Amazon EC2**

Source: National Institute of Standards and Technology[5]

3. NIST (2011). The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology.
4. *Ibid.*
5. *Ibid.*

3. Benefits of the cloud for mobile money

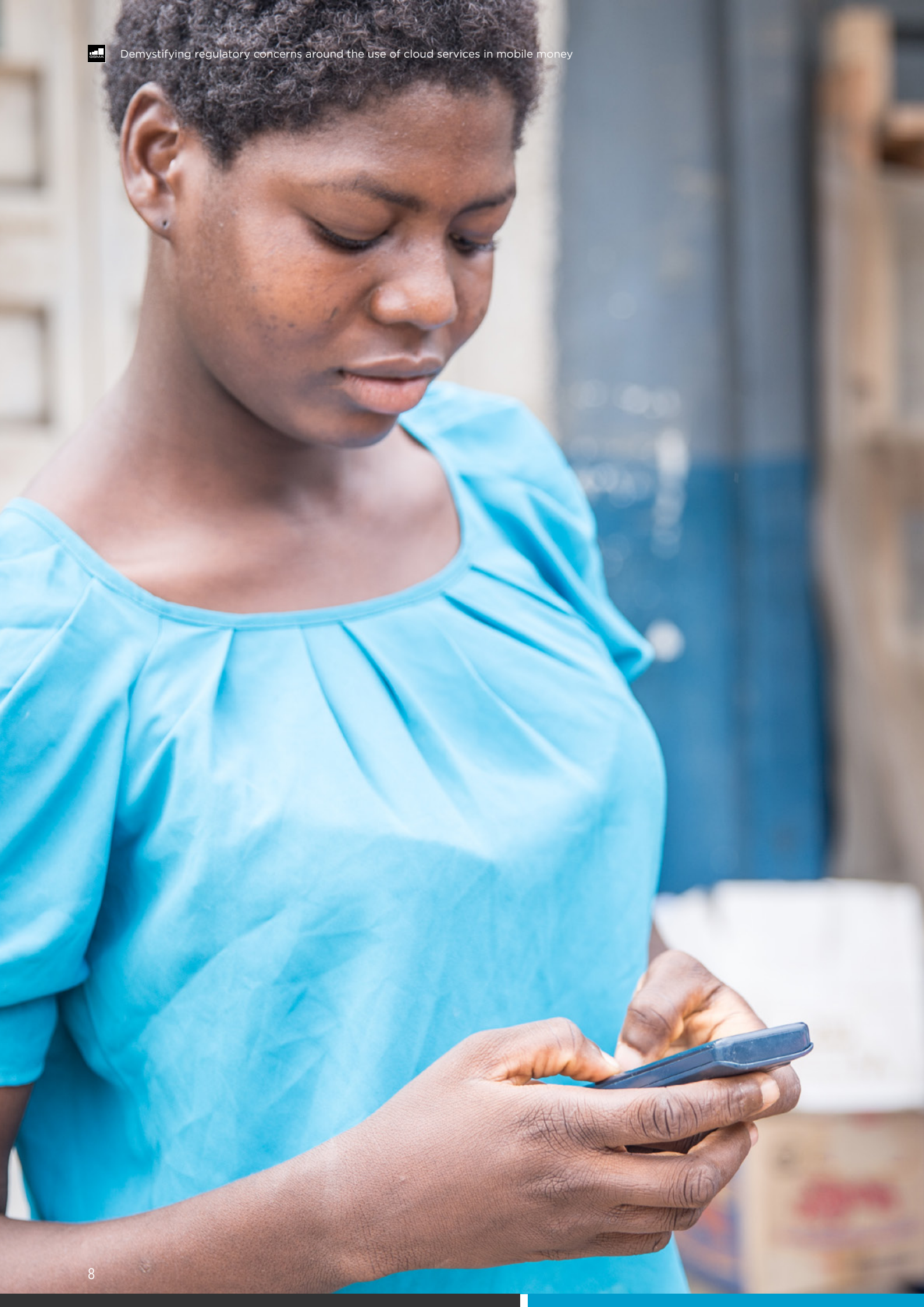
Due to its fluid and flexible nature, cloud services present several benefits over other technologies, such as on-premises data centres. Failure by the mobile money industry to take advantage of these services could severely hamper their ability to scale, and sustainably bridge the financial inclusion gap. Table 2 presents a broad overview of the benefits of cloud computing for financial services.[6]

Table 2

Benefits of cloud computing for financial services

Cost reduction	• Reduce the initial capital expenditure investment required for traditional IT infrastructure (including storing and securing data). • Leverage metering capabilities to allow for increases or decreases in capacity on demand, minimising overhead on IT expenditure.
Flexibility	• Access a shared pool of configurable computing resources. • Launch new innovation/business functions with minimal investment in supporting systems. • Change business strategy swiftly with minimal sunk costs in developing in-house data architecture.
Scalability	• Scale back office functions rapidly in response to changes in business developments. • Support organisational structure changes as well as the ability to absorb new data from outside sources.
Standardisation	• Operate uniformly with multiple outside vendor systems, as cloud technology has specific internationally acceptable standards.
Security, resilience and business continuity	• Provide efficient solutions to mitigate traditional technology risks, such as capacity, redundancy, and resiliency concerns. • Allow greater control in the management of variable IT demands, while offering new commercially viable methods to implement enhanced security controls. • Provide data recovery and business continuity mechanisms to ensure minimal service disruption of services in the case of power outages, national disasters or other emergency situations.

6. Adapted from Financial Stability Board (2019). Third-party dependencies in cloud services: Considerations on financial stability implications.



In 2019, the mobile money industry reached one billion registered mobile money accounts.[7] With over $1.9 billion being processed daily, the mobile money industry plays a key role in reaching the underserved and fostering socio-economic development.[8] The following are important benefits that cloud technology can offer to further increase the reach and efficiency of mobile money services.

Reduced costs and increased operational efficiencies

By creating secure, geographically-dispersed infrastructures, the cloud can help to increase the resilience of MMPs by expanding the capacity of their systems. Cloud services also allow MMPs to scale faster, deliver improved automation, and operate more flexibly by reducing operational costs, including initial investment and infrastructure maintenance.

Eliminated barriers to entry

In addition to lowering costs for existing providers, the use of the cloud also lowers barriers to entry for new innovators in the market. Fintechs, who are typically small and medium enterprises, can leverage the cloud to quickly scale their services in support of the mobile money ecosystem. They provide solutions that are swift and effective in meeting the growing IT demands for financial services. Today, financial service providers all over the world are increasingly using fintech solutions and have launched projects to realise cost efficiencies that these solutions enable.[9]

Ability to leverage partnerships in the ecosystem

As the mobile money industry evolves into a 'payments as a platform' approach, MMPs are introducing new business models to improve their service delivery and broaden the range of their offerings.[10] The cloud can advance this transition by enabling MMPs to collaborate with more partners globally and integrate third parties in the mobile money platform. Such efforts include partnering with third-party SaaS providers to take full advantage of cloud capabilities, and utilising the scale of fintech partners, as well as leveraging PaaS and IaaS to build up their own software as necessary.[11] This allows entities to build symbiotic relationships and increase value to all participants. Tools like big data analytics, credit scoring, artificial intelligence, and machine learning can also be leveraged effectively using international data sets, to enhance the provision of financial services without significant investments in capacity or infrastructure.

Centralised compliance mechanisms

In line with the Financial Action Task Force (FATF) recommendations on internal controls, financial organisations are required to implement group-wide programmes against money laundering and terrorist financing (ML/TF), including data sharing mechanisms.[12] To comply with this, some MMPs operating globally have invested in centralised fraud detection and Anti-Money Laundering/Counter-Terrorism Financing (AML/CFT) facilities. These facilities require cross-border sharing of information between different entities within the same group. The use of cloud can enable providers to maximise the benefits of their increased investment in centralised security measures and databases, leading to a consistent approach to security and compliance functions across the operating companies, as well as reduced costs.[13] In the next section, we look at some existing uses of the cloud in the banking sector that demonstrate the aforementioned benefits.

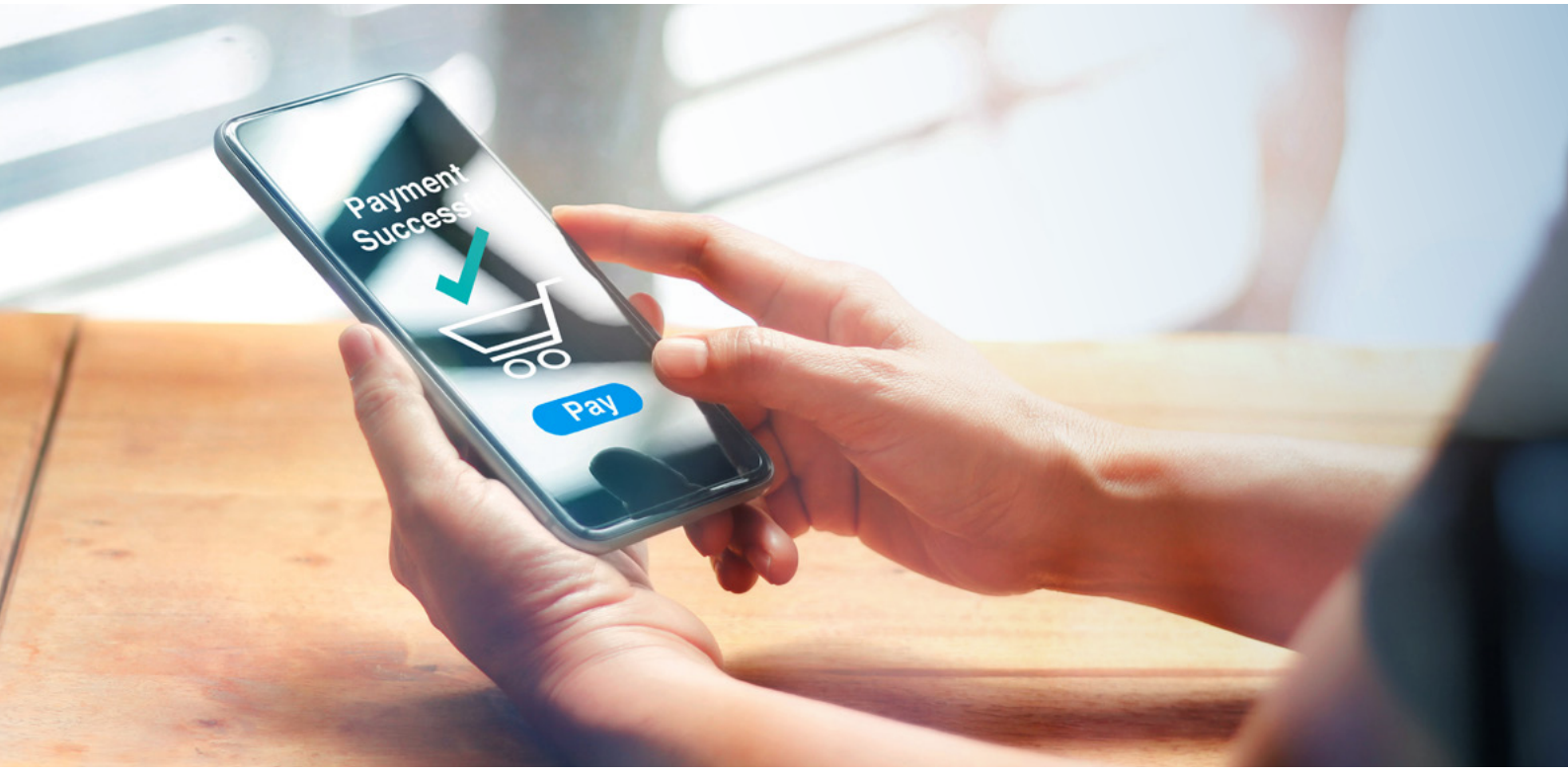
7. GSMA (2020). 2019 State of the Industry Report on Mobile Money.
8. *Ibid.*
9. European Banking Authority (2019). Final Report on EBA Guidelines on outsourcing arrangements.
10. 'The platform-based approach is not only about enlarging the ecosystem and incorporating more partners and third parties into the mobile money platform. It is about deepening engagement with individuals and businesses by offering a frictionless end-to-end experience.' GSMA (2019). Payments as a platform: The future of mobile money.
11. Broadridge Financial Solutions (2017). Pathways to Profit. Leveraging next generation technology to drive profitable growth.
12. Financial Action Task Force (2017). FATF Guidance - Private sector information sharing.
13. GSMA (2017). Cross-border data flows.

4. Digital banking on the cloud: Case studies

Judo Bank
Australia

Judo Bank is the first 'challenger' bank focused on serving SMEs financing needs in Australia, which has been granted a full banking license as an authorised deposit-taking institution.[18]

By leveraging the cloud, the bank has been able to take advantage of the investment that large cloud providers have channelled into security infrastructure. The cloud has helped the bank to apply uniform measures to the securing of data while simultaneously reducing costs.[19]



14. IT News Africa (2019). TymeBank challenges the status quo of banking in South Africa.
15. Businesstech (2019). How to build a digital bank in South Africa: it starts with a team of 180 IT professionals.
16. IT News Africa (2019). TymeBank challenges the status quo of banking in South Africa.
17. Centre for Competition, Regulation and Economic Development (2018). Digital banks: Game-changers in South Africa's banking industry?

Tyme Bank
South Africa

TymeBank in South Africa is a recently licensed bank that is fully digital and has no branches. The bank is securely leveraging cloud-based technology and aims to disrupt the industry by introducing 'simple, accessible and affordable banking' for the underserved community.[14]

The bank sits on a SaaS core banking system called Mambu which provides the new digital bank with a secure ledger for customers' accounts, managing the debits and credits incurred by customers every day.[15] With Mambu in the background, customers interface with TymeBank through its mobile friendly internet banking site and its Android app. This, coupled with its partnership with retail stores across South Africa, has allowed Tyme Bank to have tremendous success. In July 2019, the bank revealed that it had been on boarding over 100,000 customers a month due to their ability to leverage the cloud.[16]

However, TymeBank is not the only digital bank operating in South Africa. In 2017, the South African Reserve Bank (SARB) issued three new banking licences to Discovery, Bank Zero and TymeDigital. These are the first licences issued to new banks in more than a decade since the issuing of a bank licence to Finbond Mutual bank in 2001. Digital technology platforms, like the cloud have enabled entrants to overcome the high fixed and maintenance costs involved in operating bank branches and ATM networks.[17]

Starling Bank
United Kingdom

Based in the UK, Starling Bank was founded in 2014 and set itself up in opposition to other digital banking heavyweights like Monzo and Revolut. By leveraging the cloud, Starling seeks to develop intuitive user experience for all of its users.

Starling bank focussed on five key benefits of the cloud to compete against other well established banks in the market:[20]

- **Scale**: Having enough data centres and IT capacity to hold millions of customers' data.
- **Innovation**: Having the freedom to create new digital services without investing heavily in building a full IT architecture.
- **Security**: Making sure customers' data stays safe from cyber-attacks and fraud.
- **Cost**: Keeping upfront costs as low as possible to keep investors happy.
- **Regulation**: Building a completely new financial product while staying fully compliant.

18. Fintech magazine (2019). Australia's first SME challenger bank, Judo Bank, leverages technology to connect with customers.
19. *Ibid*.
20. Amazon Web Services (2018). Breaking the Banking Mould How Starling Bank is disrupting the banking industry.

5. Regulatory concerns

While access to cloud technology leads to cost savings, improved security, and increased operational resilience, concerns about the movement of data across borders can arise. These concerns are relevant, yet they may be based on misperceptions around the uses of cloud technology and can result in data localisation requirements that can have adverse implications for the mobile money industry. These measures make it difficult for MMPs to expand the reach and breadth of their services, and to integrate their operations into the wider digital financial service ecosystem.[21]

This next section presents some of the concerns for regulators around the use of cloud services, and how these can be addressed without prohibiting the use of the cloud. The table in Appendix 1 summarises this discussion.

Data privacy and security

Perceived concern:

If data is processed in countries without strong/sufficient privacy regulation in place, it could be more vulnerable to breaches, leading to violation of consumer data protection rights. These would then be difficult to enforce due to a lack of adequate frameworks. The presumption therefore, is that citizen's data is safer sitting within a country's own borders.

Addressing data privacy and security:

Data protection is not premised on the physical location of the data. The fragmentation of data by using on-premises services increases the cost of security, and limits the ability to apply uniformity to securing data. Centralised storage systems allow MMPs to better manage security and privacy. To ensure growth and innovation in the industry, a more proportionate approach is required to protect consumers. Adequate safeguards at a national or regional level will do more to protect citizens than data localisation measures.

Additionally, where there are no frameworks in place, data governance mechanisms at an organisational level can effectively address the lack of national data protection or privacy requirements. These can be premised on international standards which transcend jurisdictional barriers.[22]

National security

Perceived concern:

Government authorities have expressed concern that data held internationally may be vulnerable to surveillance by foreign governments or others.

Addressing national security:

Today, CSPs have diversified their offering to give their customers control over where their data sits geographically. This means that MMPs can avoid having their data sitting in certain jurisdictions that may not have the appropriate legal and regulatory frameworks in place.

Data can also be subjected to technical tools such as encryption and anonymisation which can substantially mitigate risks of foreign surveillance of data held internationally.

21. There are four key types of restrictions – conditional data flows, localisation and subsequent flows, localisation and indirect. The extent to which these apply will determine the level of compliance costs and the impact these will have on their organisation. GSMA (2018). Cross-Border Data Flows - Realising benefits and removing barriers.
22. National Institute of Standards and Technology (2020). NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management.

Economic impact on small and medium enterprises

Perceived concern:

The limitation of cross-border data flows may be perceived as a way to protect the national economy and local businesses. Encouragement of in-country data analysis, processing, and storage may also be viewed as a way to enhance activities at a national level and stimulate the growth of the digital economy.

Addressing economic impact on small and medium enterprises:

Data localisation requirements can have adverse effects for the development of the local economy by preventing SME players from accessing low-cost solutions. The ability to lower barriers to entry allows new fintech players to plug into the mobile money ecosystem and increase the reach and quality of services. Inability to leverage the cloud could also limit the ability of the MMPs to minimise their costs as they seek to innovate and scale, which could potentially lead to increased costs for the consumers.

Cross-border data flows enable efficient and secure provision of services, allowing MMPs to leverage security systems, skills and insights from other markets across the globe. This can then translate into greater benefits for the national digital ecosystem.

Regulatory oversight

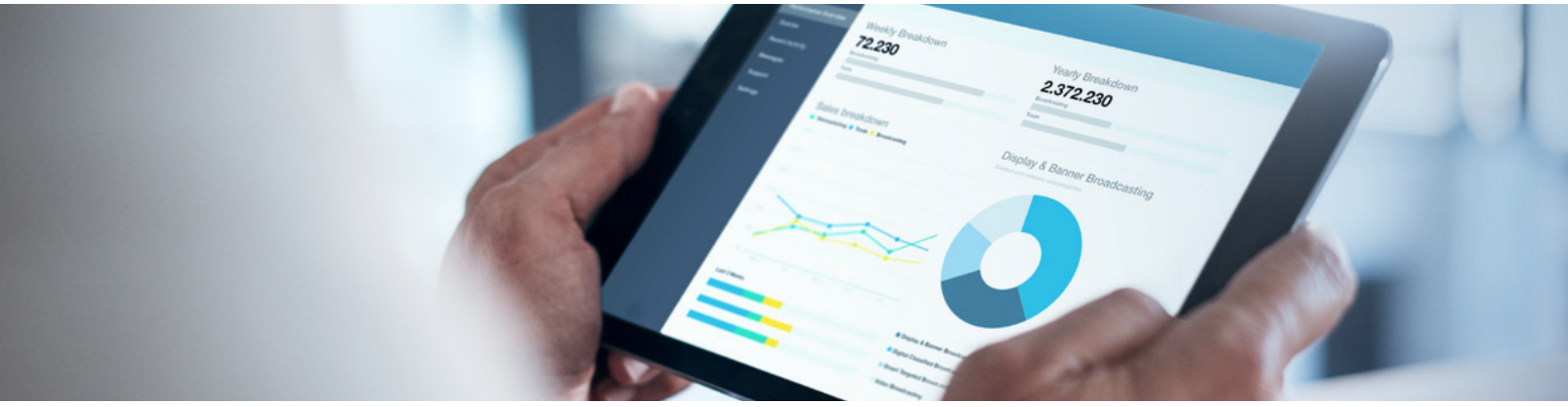
Perceived concern:

One of the key issues around the adoption of cloud is the question of the local regulators' ability to exert supervision in accordance with legal and regulatory requirements. There is a concern that data sitting outside of the local regulator's jurisdiction may impede their ability to enforce their supervisory authority over the MMP.

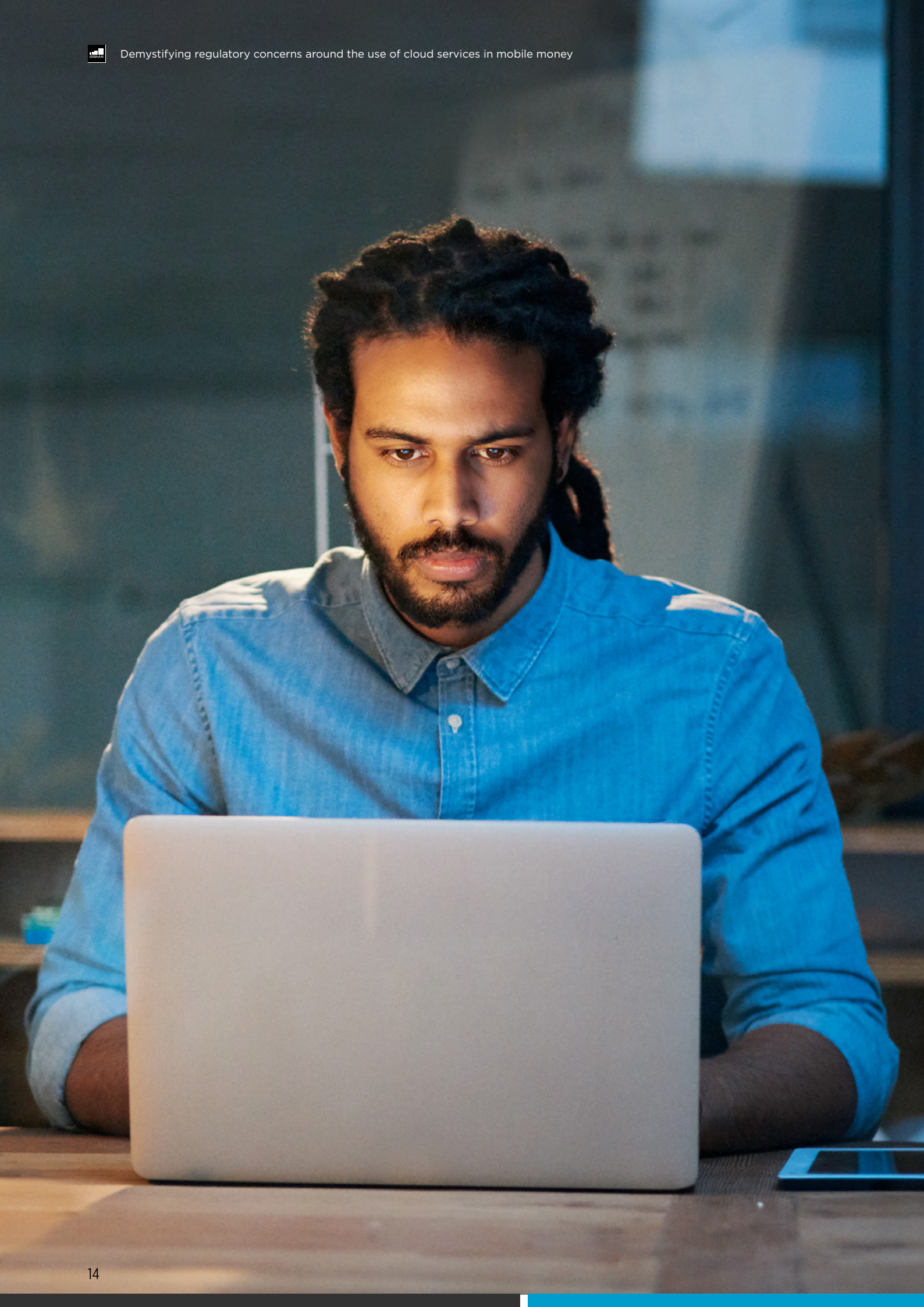
Addressing regulatory oversight:

Access and audit rights can be implemented to ensure that MMPs comply with local regulatory requirements, even if data is held in a different jurisdiction. Financial regulators need to be able to provide clear guidance on how oversight can be effectively achieved. Access and audit rights can be put into effect by the MMP with the third party service provider through contractual arrangements.

Governments can also consider multilateral provisions for the sharing of data in support of law enforcement and supervisory requirements. While such initiatives could take time, they would provide clear and predictable frameworks that give organisations legal certainty and grant authorities more direct and timely access to the offshore data they need, thereby removing the need for localisation measures.[23]



23. GSMA (2018). Cross-Border Data Flows - Realising benefits and removing barriers.



6. Implications of data localisation requirements

Where prohibitive regulation is applied to the transfer of personal data, this can present a significant burden for MMPs. Data localisation measures can impact the ability of MMPs to continue to innovate and scale securely and efficiently. The following are some of the implications of data localisation requirements for the operations of MMPs.

Increased costs

If unable to use cloud services, MMPs will need to replicate operations in each of their markets, which increases costs. This includes upgrading of hardware, and other costs related to the physical infrastructure. Costs increase further when the analysis and processing of data needs to be conducted domestically, in addition to storage. While larger players may be able to comply with these requirements, the added obligation may force smaller players out of the market.[24] Consequently, data localisation requirements can have adverse effects for the development of the local economy, and potentially lead to increased costs for the consumer.

Operational deficiencies and compromised service delivery

A fragmented approach to data storage and processing can hinder the ability of MMPs to centralise their systems, integrate seamlessly with other providers, and improve efficiencies across their operational markets. Additionally, this could impact service delivery as MMPs may be unable to provide a common user interface and user experience in all their markets.

Inability to leverage centralised systems for compliance

Data localisation requirements need data to be stored sparsely and can severely undermine data protection initiatives from the industry.[25] Centralised storage systems allow MMPs to better manage security and privacy, as well as AML/CFT measures. Fragmentation of this data can lead to improper management of data, as well as reduced incentives for investment in innovative privacy and security measures.

Uncertainty of laws

Different data localisation measures across countries increases compliance costs and complicates compliance efforts for MMPs. Additionally, it also restricts cross-industry collaboration to innovate and offer improved products and services to consumers.[26] This can act as a significant barrier, potentially deterring providers from expanding their operations into some countries and regions.

24. GSMA (2019). Data protection in mobile money.
25. GSMA (2017). Cross-border data flows.
26. GSMA (2018). Free Flow of Data Across Borders Essential for Asia's Digital Economies.

7. Overview of global practices by financial regulators

Financial regulators across the world are recognising the benefits of the cloud for the financial services industry. Outsourcing to the cloud and other third party IT services can have a positive impact on competition by facilitating entry and expansion, and increasing the ability of financial service providers to renew their IT systems in a more efficient manner. Financial regulators have a key role to play in supporting innovation and ensuring that all players can responsibly move to the cloud without compromising their responsibility of risk assurance. These are some of the approaches taken by regulators globally to provide more certainty, and support financial service providers as they move to the cloud.

United Kingdom

Financial Conduct Authority:

The Financial Conduct Authority (FCA), keen to promote innovation in the financial sector, has developed guidelines for firms seeking to adopt the use of the cloud.[27] These provide guidance to players in the financial services ecosystem such as fintechs, who have been instrumental in changing the financial landscape today, and promoting the use of cloud services. The aim of these guidelines is to set out in detail the approach to regulating firms which outsource to the cloud and other third-party IT services. Recently updated in 2019, the guidelines fall within the EU and UK legal and regulatory frameworks and provide clear understanding of the regulator's expectations. Through this, the FCA is able to ensure certain assurances are provided by the firms adopting the cloud, and sets out areas for firms to consider when outsourcing, including how they should discharge their oversight obligations.[28]

Australia

Australian Prudential Regulatory Authority:

The Australian Prudential Regulatory Authority (APRA) is another example of a financial regulator taking steps towards improving cloud adoption for the sector. APRA's prudential and reporting framework incorporates requirements and guidance regarding systems, data and operational risk management. APRA has also developed a paper which outlines prudential considerations and key principles that should be considered when using cloud computing services.[29] This was initially developed in 2015 and later updated in 2019 as the Authority recognised the growing use of cloud computing services by APRA-regulated entities, and identified new areas of weakness in their supervisory activities. The use of cloud computing services by APRA-regulated entities is expected to continue to evolve, along with the maturity of the risk management and mitigation

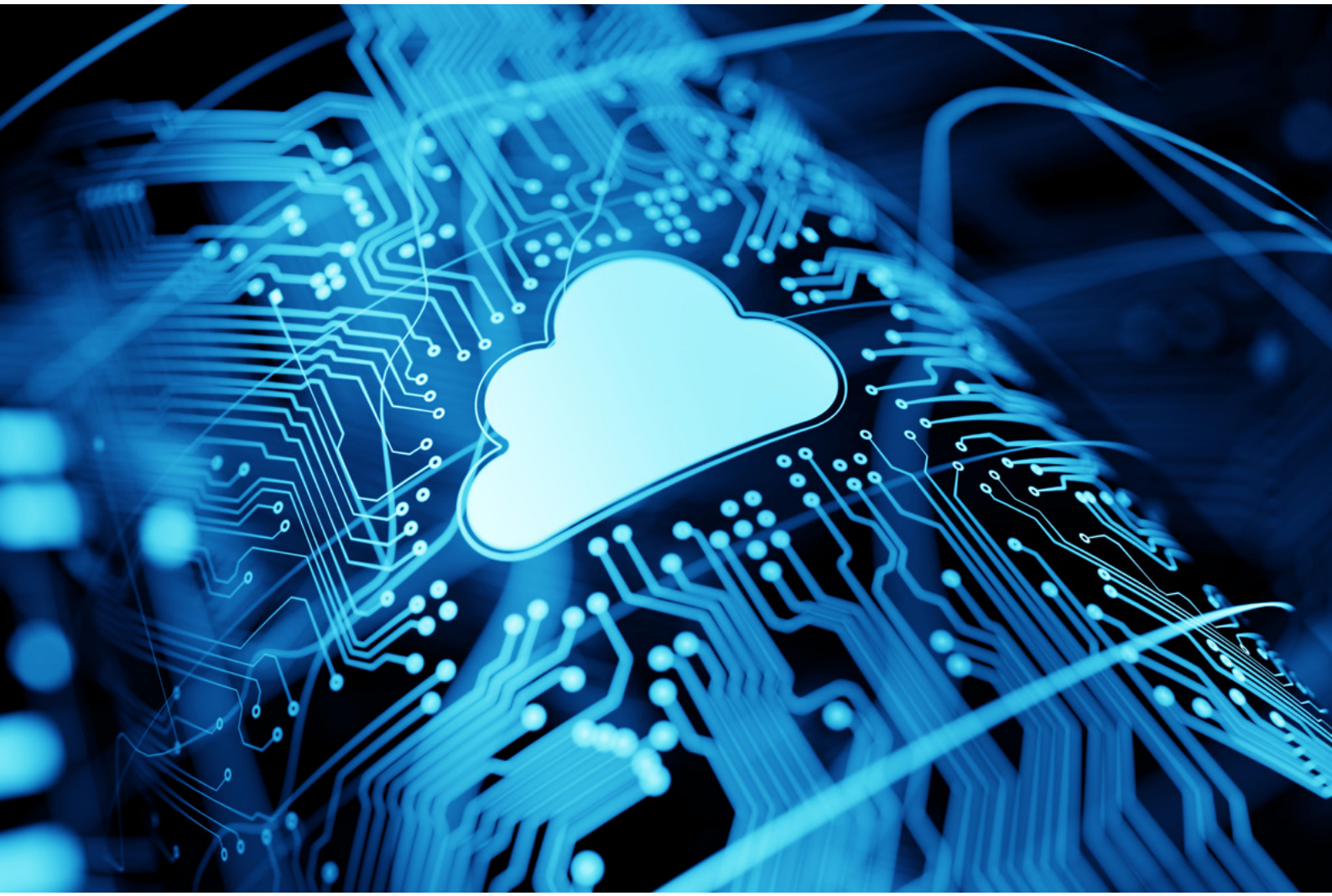
27. The Financial Conduct Authority is the conduct regulator for 59,000 financial services firms and financial markets in the UK. It is important to note that these guidelines do not extend to banks. Entities that are licenced by the Prudential Regulation Authority (PRA) will remain subject to those regulations. Financial Conduct Authority (2019). Finalised Guidance: FG 16/5 Guidance for firms outsourcing to the 'cloud' and other third-party IT services.
28. *Ibid.*
29. Australian Prudential Regulatory Authority (2018). Information Paper - Outsourcing involving cloud computing services.

techniques applied. APRA strongly supports the evolution of the financial services industry, and seeks to ensure that the risk management and mitigation techniques are strongly applied.[30]

Europe

European Banking Authority:

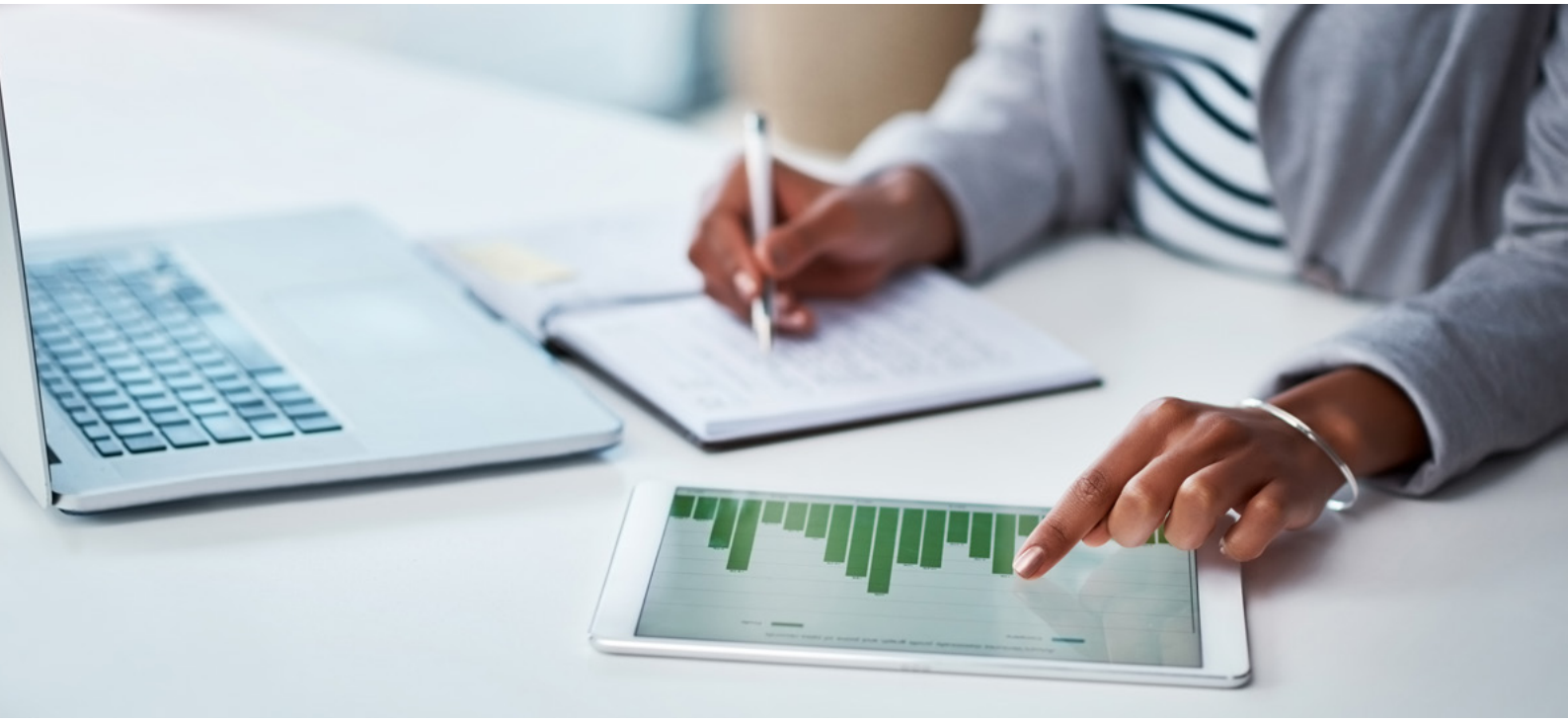
In Europe, the European Banking Authority (EBA) has recognised the need for trust in the use of financial systems, and the importance of cloud services in enabling easy access to new technologies and to achieve economies of scale. The EBA has developed guidelines on outsourcing arrangements, which provide criteria for the identification of outsourced critical or important functions that have a strong impact on the financial institution's risk profile.[31] These guidelines state that the financial institution remains responsible for the third parties' activities, and requires that sufficient resources are available to appropriately support and ensure the performance of those responsibilities, including overseeing all risks and managing outsourcing arrangements.



30. Australian Prudential Regulatory Authority (2018). Information Paper - Outsourcing involving cloud computing services.
31. These guidelines are an update from the 2006 outsourcing guidelines on outsourcing. Additionally, the recommendation on outsourcing to cloud service providers, published in December 2017, has been integrated into the guidelines. European Banking Authority (2019). Final Report on EBA Guidelines on outsourcing arrangements.

8. The role of financial regulators

Based on the above, below are some practical measures that regulators can take to mitigate the risks associated with the use of cloud technology in mobile money services while still accessing the benefits that this technology can provide.



Data privacy and security

Rather than prohibit the use of cloud services, regulators should consider undertaking a risk-based approach to privacy, which requires providers to carry out risk assessments to develop a better understanding of the risk landscape.[32] These assessments can be used to evaluate the impact of high-risk processing activities and to identify effective measures to mitigate it.

Recommendation:

- Require MMPs to carry out risk assessments regarding the privacy and security of their systems. These assessments are to be used by organisations to evaluate the impact on individuals of certain high-risk processing activities.
- Require MMPs to make these assessments available to the regulators upon request and as part of developing good accountability mechanisms.

32. GSMA (2019). Smart Data Privacy Laws – Achieving the Right Outcomes for the Digital Age.

Oversight of CSP

One of the key issues around the adoption of cloud is the question of risk and responsibility in the event of non-compliance. MMPs should be able to demonstrate adequate oversight of the CSP to ensure compliance with relevant legal and regulatory frameworks, and demonstrate accountability to their regulatory authorities on a need basis.

Recommendation:

- Implement effective supervision mechanisms, rather than restricting the use of cloud services. Regulators need to consider whether outsourcing leads to material change in the obligations of the MMP and apply supervisory measures accordingly.
- Require MMPs to be accountable for third-party relationships by adopting risk-based policies and procedures that address the level of risk posed by the outsourced activity.

Effective access to data

MMPs are generally subject to access and audit requirements by regulators as part of their legal and regulatory obligations. As highlighted above, the ability to conduct similar checks is a concern around the use of cloud services, as they are not typically based in the same country.

Recommendation:

- Develop clear requirements on access to data, including specifications on the location of data centres.
- Adopt a principle-based approach to cloud services with emphasis on accountability, rather than a prescriptive approach to dealing with access and audit requirements.

Support the development of an enabling legal and regulatory framework

Enabling cross-border data flows in a way that protects privacy can be mutually beneficial for the economy and society. Horizontal data privacy laws adopted in other countries can facilitate cross-border data flows and foster local data-driven economic activity.[33]

Recommendation:

- Engage with other relevant regulatory authorities to develop a range of cross-border data flow mechanisms.
- Ensure that data protection legal frameworks allow cross-border data flows on the basis of contractual clauses or consent.

33. GSMA (2019). Smart Data Privacy Laws – Achieving the Right Outcomes for the Digital Age.

9. The role of mobile money providers

The industry recognises that it has a role to play in ensuring that innovation is in line with regulatory requirements, and that the associated risks are sufficiently mitigated. These are some key actions that MMPs can take to mitigate the risks.

Due diligence

Outsourcing agreements do not result in the shift of responsibility to a third-party. MMPs should make extensive efforts to ensure that risk is adequately mitigated. These include understanding the characteristics of cloud services offered by third-parties prior to any significant migration.[34]

Recommendation:

- Assess the CSP's reputation, competence, experience, and flexibility of service offerings to ensure that they employ a high standard of care to the data.
- Assess the CSP's level of knowledge and readiness regarding its compliance with relevant laws and regulations.
- Ensure that all operational risks related to the outsourced activity are considered during provider selection and that proper due diligence takes place in the assessment process.

Comprehensive risk assessments

Key considerations when using cloud services are the MMP's risk appetite, long-term business strategy, and the risks arising from not using this technology. Risk assessments should therefore be carried out when collaborating with outsourcing partners, and prior to determining whether to renew the engagement.

Recommendation:

- Evaluate the potential benefits and risks involved in engaging a CSP and the strengths and weaknesses of each deployment model in the context of the business and overall strategy of the MMP.
- Conduct risk assessments that consider the benefits and risks associated with using cloud services, including operational risk, reputational risk, compliance risk, and concentration risk.[35]

34. Financial Stability Board (2019). Third-party dependencies in cloud services - Considerations on financial stability implications.
35. European Banking Authority (2019). Final Report on EBA Guidelines on outsourcing arrangements.

Contractual arrangements

Clearly outlined contractual and operational responsibilities are critical to ensure operational resilience and business continuity. By identifying these responsibilities, parties can determine how services are rendered in accordance with legal and regulatory requirements.

Recommendation:

- Develop a contract that clearly defines the expectations and responsibilities of the CSP to limit MMP liability, and mitigate disputes in the event of non-compliance.[36] Contracts should cover the following key areas:
  - Scope of services;
  - Roles and responsibilities of parties;
  - Data location and transparency;
  - Data privacy and security;
  - Audit and access rights for purposes of regulatory compliance;
  - Contingency and business continuity plans;
  - Termination procedures and data deletion/retention policies;
  - Extent of subcontractor use; and
  - Requirements for monitoring and evaluation of compliance of CSP operations.
- Ensure ongoing monitoring to manage the third-party relationship once the contract is in place. This is essential to the MMP's ability to manage the risk of the third-party relationship.

Industry standards

Industry standards are extremely important in the provision of secure services.[37] Companies operating globally need to be able to adhere to a common set of principles and standards on issues such as data privacy, security, and risk management, among others. These are important as they provide compliance even in markets where there are no legal and regulatory requirements.

Recommendation:

- Require CSPs to contractually demonstrate compliance with security measures and international standards in the form of certifications and/or security controls.

36. Office of the Comptroller of the Currency (2013). Third-Party Relationships: Risk Management Guidance.
37. ISO and NIST standards have long been recognised as the international standards for cybersecurity and data privacy. Launched in January 2020, The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management is the most recent of these standards.

Risk management frameworks

When adopting the cloud, MMPs must be able to identify potential threats and define a clear strategy on how to address them. This will include, but not be limited to, the initial comprehensive risk assessment highlighted above, and will require a holistic approach that includes key segments of the business, based on the associated risks.

Recommendation:

- Implement a holistic institution-wide risk management framework extending across all business lines and internal units and ensure that risk management measures are appropriately implemented. A good governance framework should cover the lifecycle of third-party engagements, and address the following areas:
  - Roles and responsibilities of MMP management teams;
  - Existing internal controls that mitigate known risks;
  - Business continuity plans;
  - Implementation, monitoring and management of outsourcing agreements; and
  - Exit strategies.

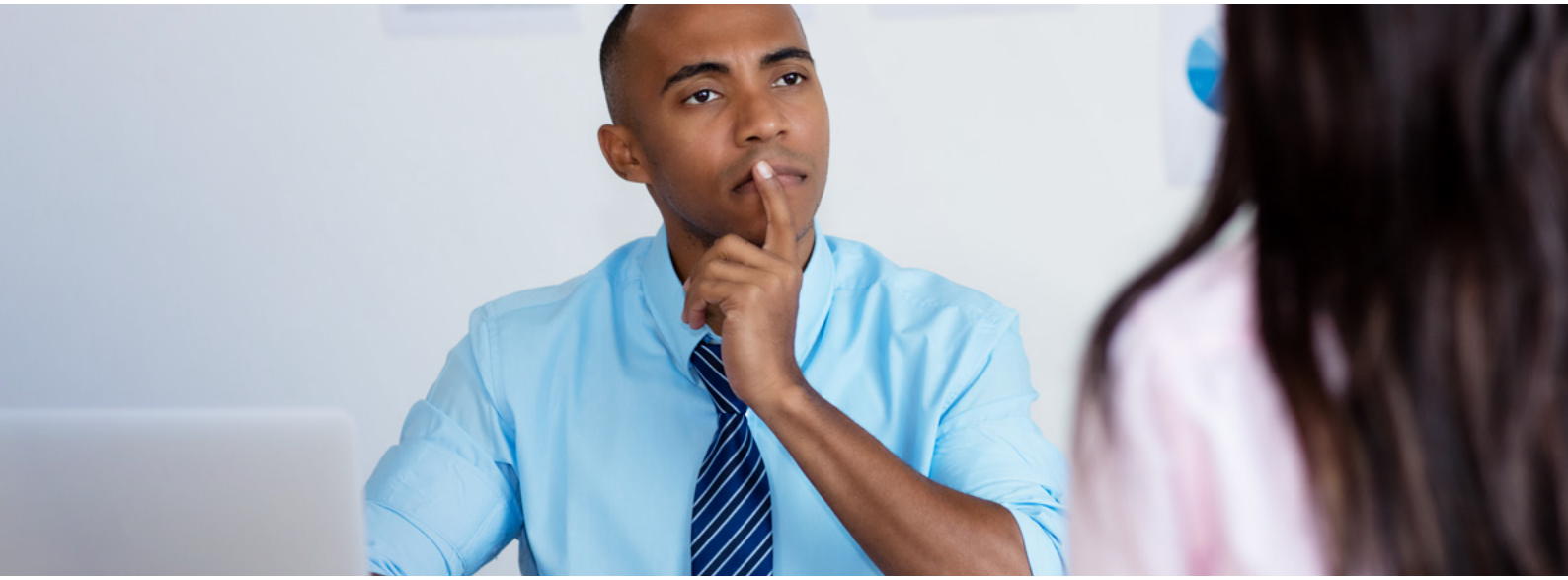
Collaboration with regulatory authorities

There is need for increased dialogue between MMPs and regulatory authorities. This is key to ensure that the regulations developed are both relevant and conducive to innovation and growth in the mobile money industry.

Recommendation:

- Collaborate with regulators to jointly develop solutions for new challenges that are beneficial for the entire ecosystem.
- Engage closely with regulators to provide the necessary assurances as they leverage the use of cloud.

10. Conclusion



Cloud services present a significant opportunity for the financial services industry, and especially for MMPs to expand the breadth and reach of their services. As the mobile money ecosystem continues to grow, so does the need to make use of new technologies and increase efficiencies while meeting consumer needs. Ultimately, restricting the use of cloud services leads to increased costs of service delivery, generates gaps in security systems, and makes it difficult for industry players to leverage global risk management and compliance programmes. Data localisation measures hamper the ability of MMPs to scale, and to integrate their operations into the wider digital financial service ecosystem.

To address this, regulators have a responsibility to ensure that uncertainty does not create a barrier to the use of cloud services in the mobile money industry by engaging with the MMPs and providing the adequate guidance. Similarly, there is a need for mobile money providers to provide relevant assurances, and demonstrate the ability to continually meet their legal and regulatory obligations when outsourcing their services to the cloud, and other third party providers. Increasingly, regulators around the world are developing guidelines on outsourcing processes that will enable the use of the cloud in a secure and efficient manner.

This report discussed the key regulatory concerns in the use of cloud in mobile money services, such as data privacy, and supervision by local regulators; and how these can be addressed without restricting the use of the cloud for MMPs. It also presented an overview of global practices by financial regulators, and provided practical recommendations for regulators and MMPs to mitigate the risks associated with the use of cloud technology in mobile money services.

The mobile money industry is constantly seeking innovative ways to meet consumer needs while safeguarding their rights and maintaining trust and confidence in the industry. There is need for closer collaboration between regulators and MMPs to effectively address any risks of emerging technologies. The GSMA remains committed to facilitate and enhance collaboration between key industry players, and welcomes all interested parties to reach out to find out more on this and other relevant topics for the mobile money industry.

Appendix 1

The demystification of regulatory concerns around the use of cloud

Regulatory concern	Addressing these concerns
Data privacy and security	
If data is processed in countries without strong/sufficient privacy regulation in place, it could be more vulnerable to breaches, leading to violation of consumer data protection rights. These would then be difficult to enforce due to a lack of adequate frameworks. The presumption therefore, is that citizen's data is safer sitting within a country's own borders.	Data protection is not premised on the physical location of the data. The fragmentation of data by using on-premises services increases the cost of security, and limits the ability to apply uniformity to securing data. Centralised storage systems allow MMPs to better manage security and privacy. To ensure growth and innovation in the industry, a more proportionate approach is required to protect consumers. Adequate safeguards at a national or regional level will do more to protect citizens than data localisation measures. Additionally, where there are no legal frameworks in place, data governance mechanisms at an organisational level can effectively address the lack of national data protection or privacy requirements. These can be premised on international standards which transcend jurisdictional barriers.
National security	
Government authorities have expressed concern that data held internationally may be vulnerable to surveillance by foreign governments or others.	Today, CSPs have diversified their offering to give their customers control over where their data sits geographically. This means that MMPs can avoid having their data sitting in certain jurisdictions that may not have the appropriate legal and regulatory frameworks in place. Data can also be subjected to technical tools such as encryption and anonymisation which can substantially mitigate risks of foreign surveillance of data held internationally.

Regulatory concern	Addressing these concerns
Economic impact on small and medium enterprises	
The limitation of cross-border data flows may be perceived as a way to protect the national economy and local businesses. Encouragement of in-country data analysis, processing, and storage may also be viewed as a way to enhance activities at a national level and stimulate the growth of the digital economy.	Data localisation requirements can have adverse effects for the development of the local economy by preventing SME players from accessing low-cost solutions. The ability to lower barriers to entry allows new fintech players to plug into the mobile money ecosystem and increase the reach and quality of services. Inability to leverage the cloud could also limit the ability of the MMPs to minimise their costs as they seek to innovate and scale, which could potentially lead to increased costs for the consumers. Cross-border data flows enable efficient and secure provision of services, allowing MMPs to leverage security systems, skills and insights from other markets across the globe. This can then translate into greater benefits for the national digital ecosystem.
Regulatory oversight	
One of the key issues around the adoption of cloud is the question of the local regulators' ability to exert supervision in accordance with legal and regulatory requirements. There is a concern that data sitting outside of the local regulator's jurisdiction may impede their ability to enforce their supervisory authority over the MMP.	Access and audit rights can be implemented to ensure that MMPs comply with local regulatory requirements, even if data is held in a different jurisdiction. Financial regulators need to be able to provide clear guidance on how oversight can be effectively achieved. Access and audit rights can be put into effect by the MMP with the third party service provider through contractual arrangements. Governments can also consider multilateral provisions for the sharing of data in support of law enforcement and supervisory requirements. While such initiatives could take time, they would provide clear and predictable frameworks that give organisations legal certainty and grant authorities more direct and timely access to the offshore data they need, thereby removing the need for localisation measures.

Glossary

Artificial intelligence	A set of technologies that seek to simulate human traits such as problem solving, perception, learning, and planning. Artificial intelligence often serves as a catch-all term for a wide-ranging set of technologies, including machine learning, big data analytics, statistical modelling, robotics process automation, natural language processing, and speech or object recognition.
Community cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations with shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third-party, or some combination of them, and it may exist on- or off-premises.
Data centre	A physical or virtual infrastructure used by enterprises to house computers, server and networking systems, and components for the organisation's IT needs.
Hybrid cloud	The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).
On-demand service	A consumer can unilaterally provision computing capabilities—such as server time and network storage—as needed automatically without requiring human interaction with each service provider.
On-premises data centre	The software and technology are located within the physical confines of an enterprise—often in the company's data centre—as opposed to running remotely on hosted servers or in the cloud.
Private cloud	The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organisation, a third-party, or some combination of them, and it may exist on- or off-premises.
Public cloud	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider.

gsma.com/mobilemoney

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601