



Regtech Adoption Practice Guide

Issue #1: Cloud-based Regtech solutions

June 2021



HONG KONG MONETARY AUTHORITY
香港金融管理局



Disclaimer

Regtech Adoption Practice Guide is a publication published by the Hong Kong Monetary Authority (HKMA). It should be noted that the sole purpose of this publication is to provide Authorized Institutions (banks) with information on the latest regulatory technology (Regtech) developments. The HKMA does not endorse any use cases, solutions and/or implementation guidance described in this adoption practice guide. If a bank intends to adopt a particular solution or implementation, it should undertake its own due diligence to ensure that the technology or approach is suitable for its circumstances.

Contents

1	Introduction	4
1.1	Background	4
1.2	Purpose	5
2	Cloud-based Regtech adoption	6
2.1	Key developments	6
2.2	How can Cloud-based Regtech solutions help Authorized Institutions?	7
2.3	Key barriers/risks of adopting Cloud-based Regtech solutions for Authorized Institutions	8
3	Implementation guidance	12
3.1	Cloud strategy and common framework	13
3.2	Tool evaluation	15
3.3	Integration	18
3.4	Cloud security	21
4	Regtech use cases	22
4.1	Use case # 1 – SaaS Regulatory Reporting Tool	22
4.2	Use case # 2 – Cloud-enabled Customer Document Review and Management platform	25
A	Appendix	27
A.1	Acknowledgements	27
A.2	Relevant regulatory requirements and/or guidance	27

01

Introduction

1.1 Background

The value of Regtech in banking is coming to the fore in Hong Kong, offering clear benefits to banks, customers and regulators. In November 2020, the HKMA released a two-year roadmap to promote Regtech adoption in Hong Kong, as laid out in a White Paper titled “Transforming Risk Management and Compliance: Harnessing the Power of Regtech”.¹ The White Paper identifies 16 recommendations across five core areas to accelerate the further adoption of Regtech in Hong Kong.

The White Paper acknowledges that since 2019, the HKMA has published a series of “Regtech Watch” newsletters, introducing banks to Regtech use cases on the adoption of innovative technology to enhance risk management and regulatory compliance. The banks interviewed for the White Paper cited these newsletters as a valuable source of information and guidance, especially the actual or potential Regtech use cases that have been rolled out or are being explored in Hong Kong or globally.

The White Paper identified 26 specific application areas of Regtech that can benefit banks. There are significant opportunities and a strong desire from the industry for the HKMA to develop and issue “Regtech Adoption Practice Guides” around these application areas.

As a successor, this Regtech Adoption Practice Guide (Guide) series builds on the “Regtech Watch” newsletters to include common industry challenges, guidance on implementation and examples of what others have done successfully to overcome adoption barriers. The Guides are to supplement other ongoing HKMA initiatives such as the Banking Made Easy initiative, Fintech Supervisory Sandbox 2.0 and the Fintech Supervisory Chatroom. Ultimately, the Guides should enhance the sharing of experience related to Regtech implementation in the industry, which will help further drive Regtech adoption in Hong Kong.

This first Guide of the series focuses on “Cloud-based Regtech solutions”. Cloud technology is a key underpinning technology behind Regtech solutions. The

¹ Transforming Risk Management and Compliance: Harnessing the Power of Regtech, HKMA (November 2020), <https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2020/20201102e3a1.pdf>

use of Cloud technology on Regtech solutions offers several benefits including timely offsite support, faster implementation and scalability of solutions. Findings from the White Paper suggest that banks that were open to using Cloud-based technology have been more successful in adopting Regtech solutions during the COVID-19 pandemic, and have therefore displayed greater operational resilience.²

1.2 Purpose

The purpose of this Guide is to provide an overview of the technology behind Cloud-based Regtech solutions, outline the common challenges observed regarding Cloud-based Regtech adoption, and share information on how others have addressed the challenges to successfully adopt Regtech solutions in their organisations. This Guide follows the outline below:

1 Explain how Cloud-based Regtech solutions can be used to support risk management and compliance

- Illustrate the benefits of leveraging Cloud-based Regtech solutions
- Describe key barriers/risks when adopting Cloud-based Regtech solutions

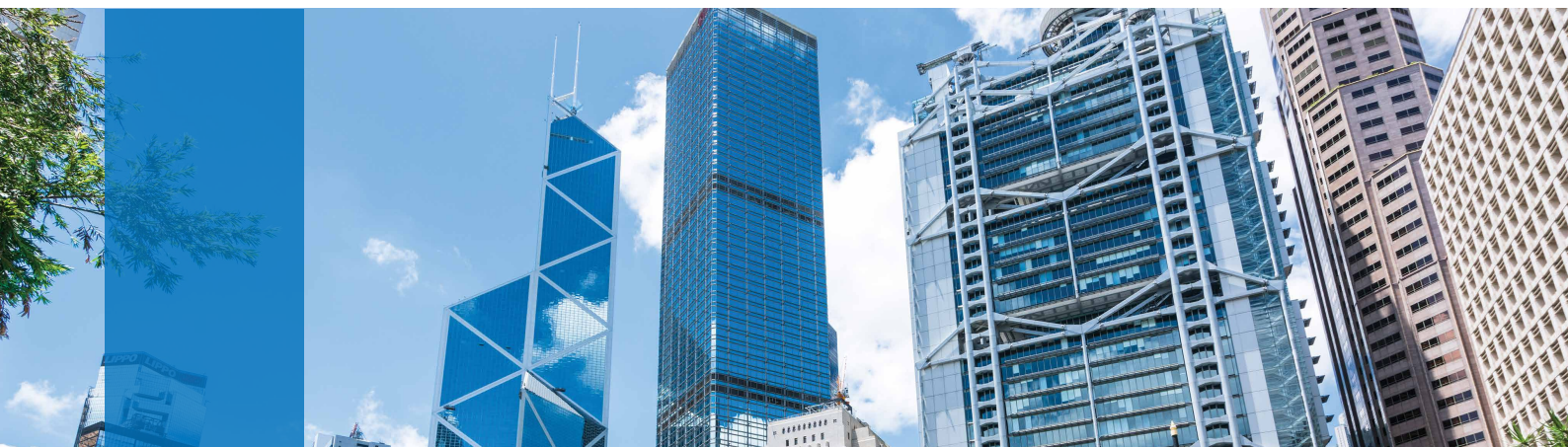
2 Provide practical implementation guidance to banks on the adoption of Cloud-based Regtech solutions

- Outline key components of Cloud-based Regtech implementation, particularly in response to the key barriers/risks of adopting Cloud-based Regtech solutions for banks
- Provide insights on what others have done to aid successful Regtech implementation

3 Share use cases on the adoption of Cloud-based Regtech solutions

- Describe the challenges faced by a bank and how the Regtech solution helped to resolve these challenges
- Outline the key learnings from successful Regtech implementation, from both the bank and the Regtech provider's perspectives

² Transforming Risk Management and Compliance: Harnessing the Power of Regtech, HKMA (November 2020), <https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2020/20201102e3a1.pdf>



02

Cloud-based Regtech adoption

2.1 Key developments

Banks are increasingly leveraging technology to drive business growth and enhance operational efficiency. Traditionally, operational requirements have been fulfilled by on-premises systems, deployed locally on a bank's own computing infrastructure.³ The acceleration of technology development is driving the incorporation of emerging technologies into banks' business and operating models. Benefits include service flexibility, enhanced customer experience, and the ability to efficiently manage risk and compliance.

Hong Kong-based banks are at different stages of Cloud adoption, with some just commencing their journey and others making continuous improvements to their established Cloud programmes. For example, a use case was showcased in the HKMA's Regtech Watch Issue No.6, where a bank utilises a Cloud-based data management platform to improve liquidity risk management.⁴ The Cloud-

based solution enables the bank to alleviate the operational risk of manual errors in data management and improve the data analytics capability.

Cloud-based technology allows banks to deploy different types of infrastructure components as a service with more flexibility and scalability, and reduce costs related to managing data and hosting on-premises infrastructure. It also allows holistic management oversight through the application of advanced analytics. The Banking industry widely accepts three service model types (Infrastructure as a Service, Platform as a Service, and Software as a Service) of Cloud. Regtech solutions exist across the three service model types. The description and common uses of Regtech under each service model are outlined in Table 1 below. Regtech enabled by different Cloud service models can offer significant benefits to banks depending on their needs.

³ The use of Cloud Computing by Financial Institutions, EBF (June 2020), https://www.ebf.eu/wp-content/uploads/2020/06/EBF-Cloud-Banking-Forum_The-use-of-cloud-computing-by-financial-institutions.pdf

⁴ Regtech Watch Issue No.6, HKMA (March 2021), <https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210319e1a1.pdf>

Table 1: Regtech solutions under each Cloud service model

	IaaS	PaaS	SaaS
Model	Infrastructure as a Service	Platform as a Service	Software as a Service
Description	A service model that provides on-demand computing, storage, and network services	A platform that facilitates development, deployment and orchestration and delivers necessary tools for development	A Cloud-based service that provides tools ranging from specific software to analytic and management tools
Regtech Application	IaaS enables centralised data (e.g. data lakes) to be used for analytics and reporting. For Regtech applications, this enables quality data inputs with smoother data identification and extraction	PaaS offers managed services for the underlying platform infrastructure, and is often adopted to lessen the need for in-house technical expertise. A platform solution can cover comprehensive areas of risk management and compliance (e.g. an outsourced platform solution to manage the account opening process)	Most market-ready Regtech solutions are SaaS-based. These Regtech solutions can be delivered over a web browser, are easy to adopt, and feature automatic updates and offsite maintenance

Risk management and compliance activities tend to be highly manual, leading to challenges around navigating, capturing, and filtering data, complex audit trails and monitoring, and limited visibility on risks and controls. To keep up with the increasing amount of data being produced and the speed of new/updated requirements in the financial sector, Regtech solutions are increasingly being developed to leverage Cloud-based technology, which provides the key infrastructure backbone when combined with technologies such as Artificial Intelligence, including Machine Learning, to allow the processing of large amounts of data to identify risks and enhance controls. Cloud-based Regtech solutions enable organisational agility to keep pace with regulatory changes, and provide greater resiliency and availability compared to traditional delivery models.

2.2 How can Cloud-based Regtech solutions help Authorized Institutions?

Enhanced mobility⁵: In general, Regtech solutions utilise technology to automate risk management and compliance processes, and enhance the monitoring process by enabling comprehensive insights developed on large amounts of data. Cloud-based Regtech solution providers can be based in a geographical location different from the users, enabling timely offsite support. Software updates for users based on regulatory changes are benefited compared

to on-premises solutions which require the bank to provide additional onsite IT support for business rule analysis and system change implementation. In addition, Cloud-based Regtech solutions deliver enhanced mobility to users, enabling access to the application at any time, from any location, and from any device with an internet connection.

Reduced costs: IT infrastructure, compliance, and risk management operations constitute a considerable portion of a bank's operational costs. If implemented correctly, Regtech can bring significant cost advantages and allow banks to focus on their core value-adding competencies.

- Regtech solutions that use Cloud-based technology allow users to retrieve data from centralised storage in a Cloud environment and save the institution the cost of establishing and maintaining its storage infrastructure. The traditionally cumbersome data extraction process from multiple siloed systems are enhanced as data is stored in a single source.
- Cloud-based Regtech solutions enable offsite solution delivery and support, helping to reduce internal system design, implementation, and ongoing maintenance costs.
- Cloud-based off-the-shelf Regtech solutions often adopt an annual subscription model, allowing organisations to more accurately estimate the total financial outlay on the solution for budgeting purposes.

⁵ Transforming Risk Management and Compliance: Harnessing the Power of Regtech, HKMA (November 2020), <https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2020/20201102e3a1.pdf>

Improved operational effectiveness: Cloud-based Regtech solutions often feature process automation and processing of large collection of data. This contributes to improved operational effectiveness including:

- **Faster response rate to new or change of regulatory requirements:** Many SaaS-based Regtech solutions are ready to be deployed with a minimal implementation and configuration timeframe. Besides, Artificial Intelligence technology with Cloud as the backbone enables automated analytics and the ability to comb through large datasets at high speed to provide more meaningful insights. It also enhances the ability to predict and react to potential risks/non-compliance against traditional monitoring and detection measures.
- **Leveraging Cloud technology,** Cloud-based Regtech solutions enable banks to scale up services swiftly when necessary, which could be more difficult to achieve using traditional on-premises technology where additional procurement is often required to scale up on-premises infrastructure.

2.3 Key barriers/risks of adopting Cloud-based Regtech solutions for Authorized Institutions

Hong Kong-based banks have started to adopt Cloud-based solutions. With the industry at a relatively early stage of Cloud adoption, foundations should be in place before

more banks will be ready to adopt Cloud-based Regtech solutions. Alternatively, we have seen Cloud-based Regtech solutions as a driver for establishing a process within organisations to adopt Cloud-based solutions to achieve benefits such as a relatively shorter timeframe to launch and tailored functionalities.

According to the findings from the 2020 HKMA's White Paper survey, security and regulatory needs, such as data protection and network security, are top considerations for a bank when evaluating Cloud solutions. Most of the key potential barriers to Cloud-based Regtech adoption cited by banks focus on the general adoption of Cloud-based solutions. **Section 3** of this Guide ("**Implementation Guidance**") will further explore the methods banks have adopted to overcome the barriers and mitigate or minimise the impact of key risks.

Key barriers

- **Company policy and governance:** An enterprise-level Cloud assessment framework should be put in place for organisations to evaluate the suitability of Cloud-based solutions. Without a clear framework or governance structure to evaluate Cloud-based solutions, management may take a more conservative/risk-averse view towards the adoption of Cloud-based technology.



It is unlikely that the head office will give the green light on the use of Cloud-based Regtech solutions because they have not yet launched it in their home jurisdiction.

We need to study (Cloud-based Regtech solutions) before changing our existing policies/risk appetite.



Source: 2020 HKMA's White Paper survey for Authorized Institutions, KPMG Analysis



Without an enterprise-level Cloud assessment framework, it is less likely that Cloud-based Regtech solutions will be adopted by business users.

- **Insufficient capability and experience:** Organisations lacking sufficient expertise and experience related to Cloud-based technology will find it challenging to establish proper governance, management, controls, and support to adopt Cloud-based Regtech solutions.

“



The most critical challenge is the lack of well-rounded talent with sound understanding of technology risk and regulatory requirements for different jurisdictions in the region.

Source: 2020 HKMA's White Paper survey for Authorized Institutions, KPMG Analysis

”



- **Legacy systems:** Many banks still possess legacy systems that are tightly coupled to existing infrastructure and inflexible to changes. The adoption of a new Cloud-based Regtech solution leads to the modernisation or full replacement of existing applications or systems.

Organisations need to budget time and effort on data migration depending on the size and complexity of the current process and scale of the Cloud-based Regtech solution.

“



.... A key barrier would be the integration of Cloud-based solutions within an in-house environment.

Source: 2020 HKMA's White Paper survey for Authorized Institutions, KPMG Analysis

”

Key risks

According to the findings from the HKMA's White Paper survey, banks are hesitant to adopt Regtech solutions because of key risks around data and security. Furthermore, the lack of IT governance, complex compliance issues, and potential vendor lock-in are also among the risks that contribute to slow Cloud-based Regtech adoption rates.

It is important to understand the key risks around adopting Cloud-based Regtech solutions, which is the first step towards evaluating and eventually adopting Cloud-based Regtech solutions. In this section, we list some common key risks observed from the industry on Cloud-based Regtech adoption:

- **Insufficient IT governance model and control:** Business users adopting Cloud-based Regtech solutions without fully understanding the underlying Cloud technology could lead to insecure or unauthorised Cloud services as part of the bank's IT environment. This indicates a lack of organisational Cloud governance and control, and creates cybersecurity risk (e.g. common internet-based attacks and Cloud-specific attacks) as well as risks related to non-compliance (e.g. the Personal Data (Privacy) Ordinance (PDPO) violations). Inadequate third-party monitoring can also result in lack of understanding and over-reliance on third-party Cloud providers, which could increase data security risks.



“



The Company is sitting on the fence since there are challenges with Regtech adoption, such as difficulties in ensuring information security, data privacy and protection, the evolving regulatory landscape, and legacy IT systems.

Source: 2020 HKMA's White Paper survey for Authorized Institutions, KPMG Analysis

”

- **Compliance across jurisdictions:** There is a risk of non-compliance with data storage or transmission requirements where multiple jurisdictions are involved (e.g. a Hong Kong-based bank is using a Cloud-based Regtech solution where the Cloud data centre is located in the European Union), as many different jurisdictions and industries have varying regulatory requirements (e.g. the PDPO and General Data Protection Regulation). Banks operating in different regions should observe the related data sovereignty/residency laws of the jurisdictions.

As some Cloud service providers may operate in multiple locations, under disaster recovery (DR) scenarios, if a Cloud service provider does not have a DR site in an approved location, there is a risk that data may flow to other jurisdictions and cause a compliance breach.

- **Data protection and disaster recovery:** Cloud-based applications and platforms create complexity of data protection and DR. Organisations need to be cautious about the applicable regulations on data access rights and need to assess if the Cloud-based Regtech provider

will allow a third-party Cloud vendor to access sensitive customer data.

Organisations should put in place proper DR plans for Cloud-based applications and platforms, whether it is provided by the Cloud provider's underlying DR strategy (e.g. multiple data centres and cross-regional resilience), another Cloud vendor (i.e. multi-Cloud) or the organisation's on-premises DR site. The organisation should keep the on-premises and Cloud environments secure and meet relevant regulatory requirements.

- **Vendor lock-in:** Organisations are at risk of data loss if their vendor's exit strategy is not fully planned out prior to the commencement of the contract. It is important to understand the available methods and time period given to retrieve data in the event of contract termination. The organisation should evaluate if the period provided is sufficient to transfer the data back in-house or to another vendor's solution. The risk is not limited to the exiting vendor relationship. It also applies to the method used to transfer data to other platforms when required.



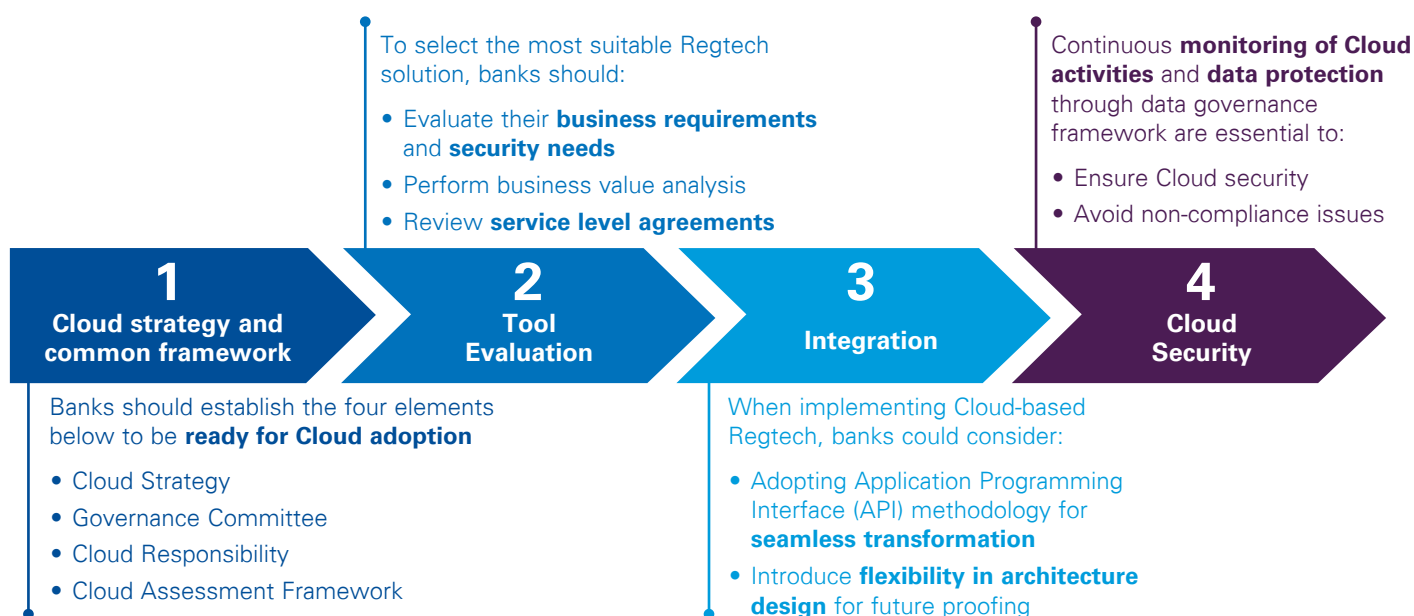
03

Implementation guidance

Given all the benefits that Cloud-based Regtech solutions bring, the introduction of various Cloud service models (e.g. SaaS, PaaS, IaaS) and deployment models (e.g. private, hybrid, public, multi-Cloud) can be complex as each model brings different risks and challenges. As a prerequisite for Regtech adoption, banks need to gain a clear understanding and develop Cloud capabilities in order to establish robust guidelines and an enterprise-level framework to assist with implementation.

This section outlines some key components of Cloud-based Regtech implementation (please refer to Figure 1 for an illustration), particularly in response to **section 2.3 (“Key barriers/risks of adopting Cloud-based Regtech solutions for Authorized Institutions”)**. This section is not an exhaustive guide to Cloud-based Regtech implementation. Rather, it provides observations on what others have done to aid successful Regtech implementation.

Figure 1: Key components of Cloud-based Regtech implementation



Readers may also refer to relevant regulatory requirements and/or guidance in Hong Kong for actual implementation in the Appendix A.2 (not intended to be exhaustive).

3.1 Cloud strategy and common framework

Banks need to have clear enterprise-wide guidelines on Cloud adoption in order to facilitate Cloud-based Regtech adoption. Banks that are ready for Cloud adoption usually have established relevant Cloud governance such as a Cloud strategy, Cloud migration framework, and Cloud assessment framework.

3.1.1 Cloud strategy

To develop a Cloud strategy, organisations should first understand their current landscape and future priorities. The current landscape includes assessing the organisation's enterprise architecture and internal resource capabilities. Future priorities should align with the organisation's vision and strategy. Banks should form their own entity-specific Cloud strategy that aligns with their current culture, business vision, and capabilities. Once organisations have determined their Cloud strategy, this can be applied as lens to evaluate Regtech solutions.

The purpose of this implementation guide is to share guidance on Cloud-based Regtech implementation. As the absence of an overall Cloud adoption framework has been identified as a key barrier to adoption, the key components of a Cloud strategy are outlined below:

- **Vision and principles:** The organisation should be guided by a vision, for example "to transform to achieve agility and speed to market". This can be achieved through reviewing existing strategy and operating model documents, running a "Cloud visioning Design Thinking workshop" designed to understand the company vision and the key organisational drivers for Cloud adoption through gathering senior management (e.g. heads of business units and C-level executives). Organisations can also perform a gap analysis on the existing practice and the vision, and formulate guiding principles on Cloud strategy.

- **Deployment model:** Common deployment models, including private, public, hybrid, and multi-Cloud, demand different levels of governance, controls, and internal technical support. Based on a bank's current landscape (e.g. architecture constraints and risk acceptance culture), a bank can determine the deployment model that is best suited for the organisation. This will then determine the type of Regtech solutions the organisation will adopt in the future. An overview of the four deployment models is outlined below:

- **Private Cloud:** A private Cloud consists of Cloud infrastructure used exclusively by a single organization. The exclusivity to the Cloud suggests higher levels of control and privacy. The benefits of a private Cloud also include the flexibility of tailoring the service to meet specific IT requirements. It requires a higher setup cost for the Cloud infrastructure as compared to other deployment models.
- **Public Cloud:** This is the most common type of Cloud deployment model with the Cloud resources delivered over the internet and open for public use. All components of the Cloud infrastructure are owned and managed by the service provider. There is limited flexibility to meet specific requirements and may require additional security measures. The public Cloud, however, provides higher reliability and scalability as compared to private Cloud due to the vast network of servers. Another benefit is the lower costs as organisations only pay for the service used.
- **Hybrid Cloud:** A hybrid Cloud is a composition of a private Cloud (or on-premises infrastructure) and a public Cloud. The combination allows users to take advantage of the benefits from both. Banks are able to store more sensitive data on the private Cloud to meet specific regulatory requirements and operate other functions on the public Cloud. This gives organisations greater flexibility around deployment and enables cost savings on infrastructure. The set-up of network connections could be complicated, which requires careful planning to manage any potential security risks associated with the bank's IT environment.

- **Multi-Cloud:** Although the name may suggest a similar characteristic as the hybrid Cloud, a multi-Cloud uses a number of different public Clouds to host the data. Organisations may choose to use private Cloud as well, but the focus for multi-Cloud is on utilising various public/private Cloud solutions for different services. It allows users to choose the service from different providers depending on their specific needs (e.g. service type and data location requirements).
- **Governance and organisation:** The Cloud strategy should consider the governance and organisation of Cloud capabilities within a bank. Both business and IT are required to understand the business value that a Regtech solution brings, assess its suitability to the organisation against a pre-defined framework, and follow the established processes to gain internal approval. To fully understand and evaluate Cloud solutions, different departments within a bank (e.g. business, compliance, legal, finance, and IT departments) need to come together to form a comprehensive picture of the strategy, access controls, contingency plans, and data location, etc. The purpose of a Governance Committee is to ensure that all necessary support is in


place, prioritise points of transformation per the Cloud strategy, and provide a single point of decision and control. Some banks have also established a central Cloud Centre of Excellence to lead development, research, and centralised guidance on Cloud-based implementation.

3.1.2 Establish governance and framework

Cloud responsibility: As processes, infrastructure, and applications are being moved to the Cloud to enable integrated compliance and risk management, there is a need for banks and Cloud service providers to have clearly defined responsibilities for each part of a solution or process. A clear model of sharing governance and responsibility can help prevent misunderstandings between parties (An example is shown in Figure 2. The definition of a shared Cloud responsibility model may vary across different Cloud service providers). Although the Cloud provider has responsibility over certain areas, banks should still perform independent assessments on those areas to ensure that they are compliant with all the applicable regulatory requirements and/or guidance (Appendix A.2).

Figure 2: Sample shared responsibility model between the bank and Cloud service provider

Shared Cloud responsibility model				
	On-premises	IaaS	PaaS	SaaS
Application	●	●	●	●
Data	●	●	●	●
Runtime	●	●	●	●
Middleware	●	●	●	●
Operating System	●	●	●	●
Virtualisation	●	●	●	●
Networking	●	●	●	●
Storage	●	●	●	●
Servers	●	●	●	●

 User responsibility
  Cloud provider responsibility

Source: Various Cloud Service Providers

Cloud assessment framework: A governance process should be put in place to assess the Cloud solutions from different angles (e.g. security and reliability) as well as Cloud migration initiatives. Cloud-based solutions that do not meet security standards could expose organisations to significant financial implications and different risks such as reputational risk. However, excessive rules increase the administrative effort and may end up stifling the business benefits that a Regtech solution brings, such as speed to market and cost effectiveness. The key is to strike the right balance.

The following industry bodies have produced frameworks to assess Cloud-based solutions. Some organisations have used the following as a base to develop an assessment framework:

- Information Security Forum⁶
- Information Systems Audit and Control Association⁷
- Cloud Security Alliance⁸

Regtech firms that have the following data security and protection-related certifications (not intended to be exhaustive) could enable banks to further evaluate the suitability of the Regtech solution:

- **ISO/IEC 27001:** Information Security Management
- **ISO/IEC 27017:2015:** Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- **ISO/IEC 27018:2019:** Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- **ISO/IEC 20000:** IT Service Management System
- CSA Security, Trust, Assurance, and Risk (STAR) Registry
- **SOC 2 TYPE II:** Report on controls at a service organization relevant to security, availability, processing integrity, confidentiality or privacy
- **SOC 3:** Trust services report for service organizations

3.2 Tool evaluation

When ready to adopt a Cloud-based Regtech solution, the bank should evaluate different areas (e.g. business requirements, different approaches, security and privacy standards) and perform due diligence on the tools and vendors to choose the most suitable solution. Furthermore, to optimise their Regtech investment, banks should take a risk-based and value-driven approach. It is important that the risk management framework should support the strategic direction of the organisation.

3.2.1 Framework

A tool evaluation framework is necessary and an established process, which should contain the following key elements, should be followed:

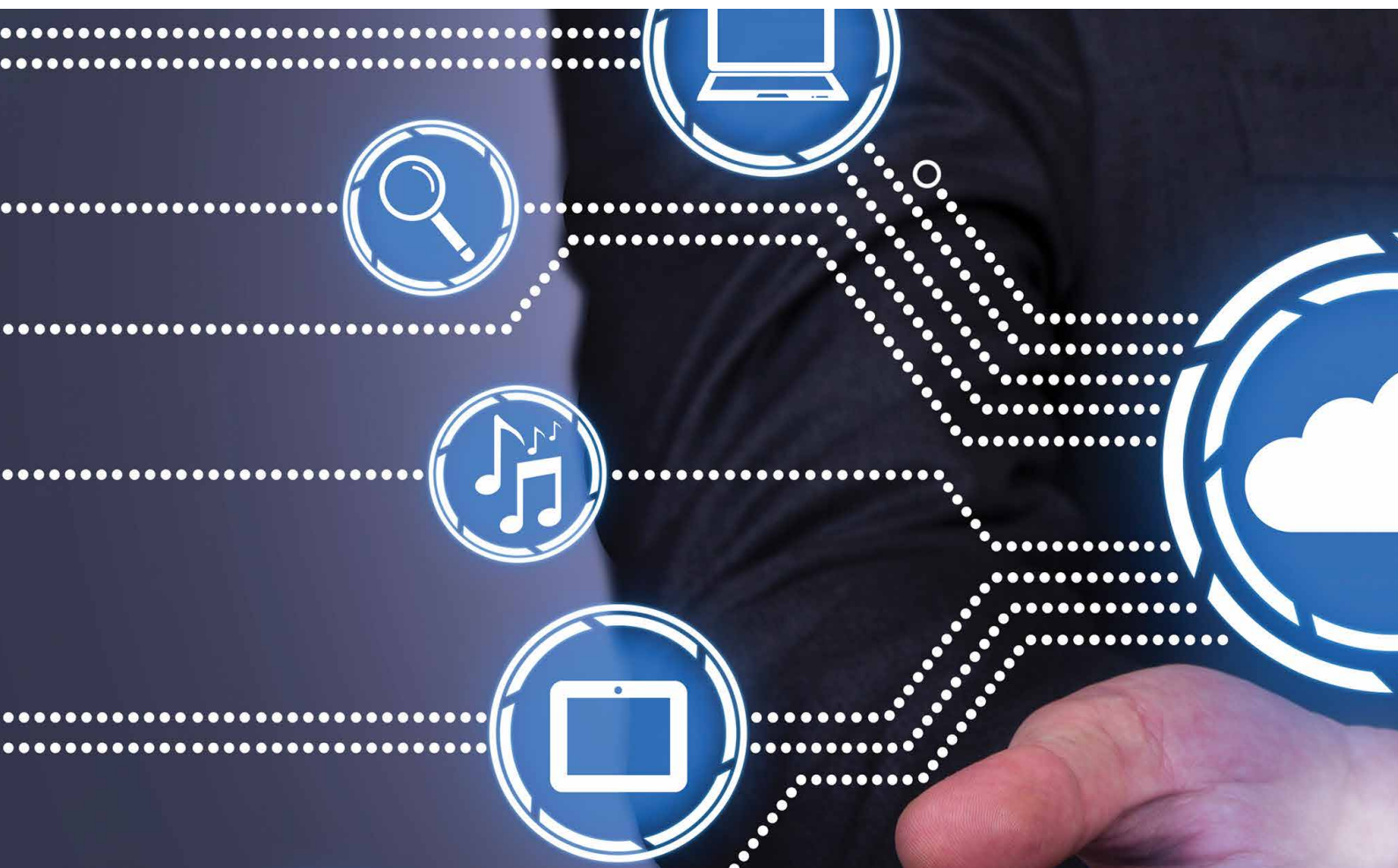
- **Business value:** The bank should validate that a business need exists and a technology solution will bring value to the institution (e.g. through a Cost & Benefit analysis, and Return on Investment).
- **Solution strategy and scoping:**
 - Banks should first develop a solution strategy to align the strategic purpose with their overall vision, identify key values and objectives, and outline some guiding principles for selection and implementation.
 - It is also important to identify in-scope functional areas and processes for evaluation and determine current state functional priorities and pain points in order to determine the functional fit of the solution. Banks should identify their unique business practices and convert them to requirements to build an initial list of solution requirements. Once the list is completed, banks could conduct a high-level assessment of solutions based on functional and strategic perspectives and develop a shortlist of potential solutions.
 - Lastly, banks should finalise internal resource allocations and establish a programme governance structures stating the timeline and expectations.

⁶ Using Cloud Services Securely: Harnessing Core Controls, Information Security Forum (November 2019), <https://www.securityforum.org/solutions-and-insights/using-cloud-services-securely-harnessing-core-controls/>

⁷ Cloud Risk – 10 Principles and a Framework for Assessment, ISACA (September 2012), <https://www.isaca.org/resources/isaca-journal/past-issues/2012/Cloud-risk-10-principles-and-a-framework-for-assessment>

⁸ Cloud Controls Matrix v3.0.1, Cloud Security Alliance (August 2019), <https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v3-0-1/>

- **Solution evaluation:** The necessary steps include issuing the Request for Proposal (RFP) to the vendors, preparing for evaluation, and assessing the solutions. Banks should prepare for an evaluation by tailoring selection criteria and materials. Typical categories to consider include:
 - **Solution and needs:** This includes whether the solution can support the business processes, solution adaptability, experience of the vendor (including subject matter expert and regulatory-related capabilities) and customer support provided.
 - **Vendor company due diligence:** This includes the financial status and ability of the service provider to meet service commitments, the location of the data centre and its suitability to a bank based on rules and regulations, whether the vendor complies with relevant regulations and standards, the appropriateness of a vendor's internal controls covering security and privacy standards, sub-contracting, and system vulnerability assessments.
- **Solution selection:** After completing the vendor evaluations, the banks need to develop solution recommendations and finalise the solution selection process. The banks should compare the solution functionality and costs. Each solution's fit with the overall solution strategy should be assessed and the functionality should meet/exceed the requirements. The best-fit solution should then be recommended to the programme leader to finalise the solution selection. After selecting the preferred vendor, the bank should create an implementation strategy to examine how the solution can be integrated into their current system regarding security architecture, cost of operation and ongoing maintenance, etc. The bank can suggest alterations to the vendor proposals and discuss any specific integration and security requirements.



3.2.2 Cloud-based Regtech adoption examples

Outlined below are some commonly seen Cloud-based Regtech solutions and the organisational value drivers that lead to adoption. In each scenario, the solution is applicable under both on-premises and Cloud models. Banks should take their Cloud strategy into consideration when determining which solution is the most appropriate.

- Off-the-shelf Cloud-based Regtech solutions:** This refers to SaaS products that provide a targeted solution to address specific risks or compliance pain-points. The underlying Cloud infrastructure is managed and controlled by the vendor, and the organisation has limited control over system features and functions other than user-specific configuration settings.⁹ This type of solution will suit situations that value agility above control as the solution can be evaluated, integrated, and set up in a short period of time. If the bank decides to switch the solution later on, a Cloud-based
- Hybrid platforms comprising both in-house solutions and outsourced Cloud-based Regtech solutions:** An organisation may already have a system in operation and seek to adopt a Regtech solution as an add-on tool to optimise specific areas. For example, an organisation's Governance, Risk and Compliance (GRC) system operates with a team that manually updates the obligation inventory. The organisation can choose to adopt an obligation register Regtech solution and integrate it into its existing GRC platform to automate this particular process. This method provides the bank with some degree of control and stability, while improving efficiency and effectiveness in certain areas.

⁹ Software-as-a-Service Quick Reference Guide, KPMG International

¹⁰ Opara-Martins, J., Sahandi, R. & Tian, F. Critical analysis of vendor lock-in and its impact on cloud computing migration: a business perspective. J Cloud Comp (April 2016), <https://doi.org/10.1186/s13677-016-0054-z>



- **Customised Regtech platform solutions:** Banks that have a heightened focus on stability, control, and consistency can adopt customised Cloud-based Regtech solutions to reinvent their compliance and risk management functions. A platform that integrates compliance and risk management data across the bank enables advanced and predictive analytics to be applied at the organisational level. Going further, application systems hosted on the Cloud, with fully integrated and modular systems, enable near real-time responses to risk and regulatory changes. The solution can be built fully in-house or the bank can source the base solution from a vendor and go through system implementation with custom configurations and integration into the bank's IT infrastructure. The bank should determine if it has the skillset available internally to support the transformation, or if there are gaps that need to be filled via training or external hires.
- **Data protection:** In order to protect data, banks need to classify the data being processed and produced by the Regtech solution. Data classification allows banks to assess the type, sensitivity, and criticality of the data based on regulatory compliance, best practice, and organisational needs. When entering into an outsourcing agreement with the service provider that operates in overseas jurisdictions, banks should evaluate the relevant risks, taking into account the legal systems and regulatory regimes of the overseas jurisdictions.¹¹ Banks should ensure the data is secured and accessible for daily operation, contingency, or DR.
- **Disaster recovery considerations:** Banks should include the Cloud-based Regtech solution in the organisational DR plan prior to its launch. Per any DR plan, the Regtech solution needs to be subject to a risk assessment and business impact analysis, and full testing needs to be conducted on the DR response. Some banks may choose to adopt a hybrid Cloud model, where both private and public Cloud infrastructures are used in the organisation. A hybrid Cloud model could more easily meet both regulatory and DR requirements as it involves the replication and encryption of data in the private Cloud network before it is sent to a DR site. However, this approach requires the alignment of the organisation's overall Cloud strategy, and can include significant investment in enterprise IT infrastructure and capabilities.

3.2.3 Contractual considerations

Some Cloud-based Regtech solutions (e.g. off-the-shelf products) could reduce direct control and visibility into security, availability, and confidentiality elements. Prior to contracting with solution vendors, banks should review and evaluate a number of components of the service level agreements, especially around data protection and storage. Below are the components that are most applicable to Cloud-based Regtech solutions:

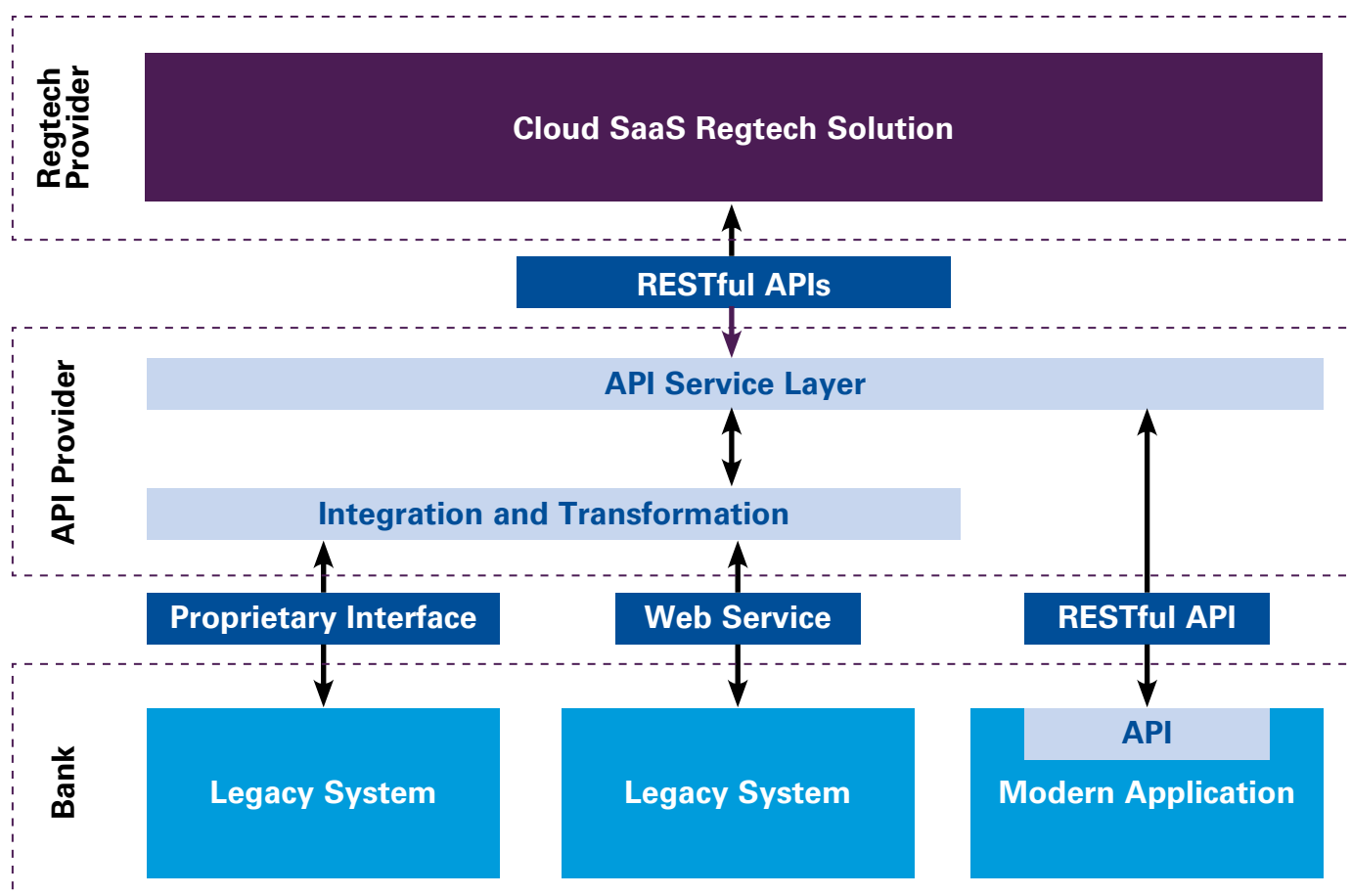
- **Data portability:** Data portability defines what kind of data the bank can extract from the Cloud once the Cloud subscription expires. This evaluation will be particularly helpful to assess the flexibility and control with regards to data transfer between Cloud solution providers and banks. In the event of exiting the service contract, the banks should lay down an exit plan with the vendor to formulate a clear data deletion procedure and consider the transferability of the outsourced service.
- **Data sovereignty:** Banks should understand where vendors store and control their data for compliance purposes. This is particularly challenging for banks that are considering implementing a multi-Cloud model as they should align different requirements from multiple Cloud vendors and adhere to the local legal requirements of each jurisdiction.

3.3 Integration

Legacy infrastructure was designed for stability, reliability, and auditability. However, in the HKMA's White Paper survey, 37% of banks in Hong Kong noted it as a major barrier to Regtech adoption since "complex legacy infrastructure renders solution development and implementation challenging".¹² These banks could consider using API methodology to create an abstraction layer between the legacy system and the Regtech solution. An API is a computer programming approach for facilitating exchange of information and executing instructions between different computer systems¹². APIs enable integration of internal and external systems running on-premises and delivered via Cloud, allowing banks to harness the power of Regtech without going through a major transformational overhaul. A simplified API reference architecture is shown in Figure 3 to illustrate how a Cloud-based Regtech solution could be integrated with a legacy system by applying an API service layer.

¹¹ HKMA Supervisory Policy Manual: SA-2 Outsourcing <https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf>

¹² Transforming Risk Management and Compliance: Harnessing the Power of Regtech, HKMA (November 2020), <https://www.hkma.gov.hk/media/eng/doc/key-information/press-release/2020/20201102e3a1.pdf>

Figure 3: Simplified API reference architecture¹³

Source: KPMG

As indicated in Figure 3, the API Provider layer helps to connect multiple applications and sources from the bank into a single touchpoint that can be easily connected to the Regtech providers. The layer also mediates the requests and controls which APIs can be accessed by the Regtech providers. To minimise changes required by existing

banking systems in exposing interfaces to the Regtech solution, the API provider can utilise a variety of methods to integrate and transform the data model between the API Service Layer and existing systems. Figure 4 outlines the suggested practice guidance on API implementation.

¹³ Proprietary interface and Web Service are used to exchange structured information in computer networks based on communication protocol specifications. RESTful API (Representational State Transfer API) is an architectural style for an API. Collectively, they represent different communication protocols used between a legacy system and the API provider.

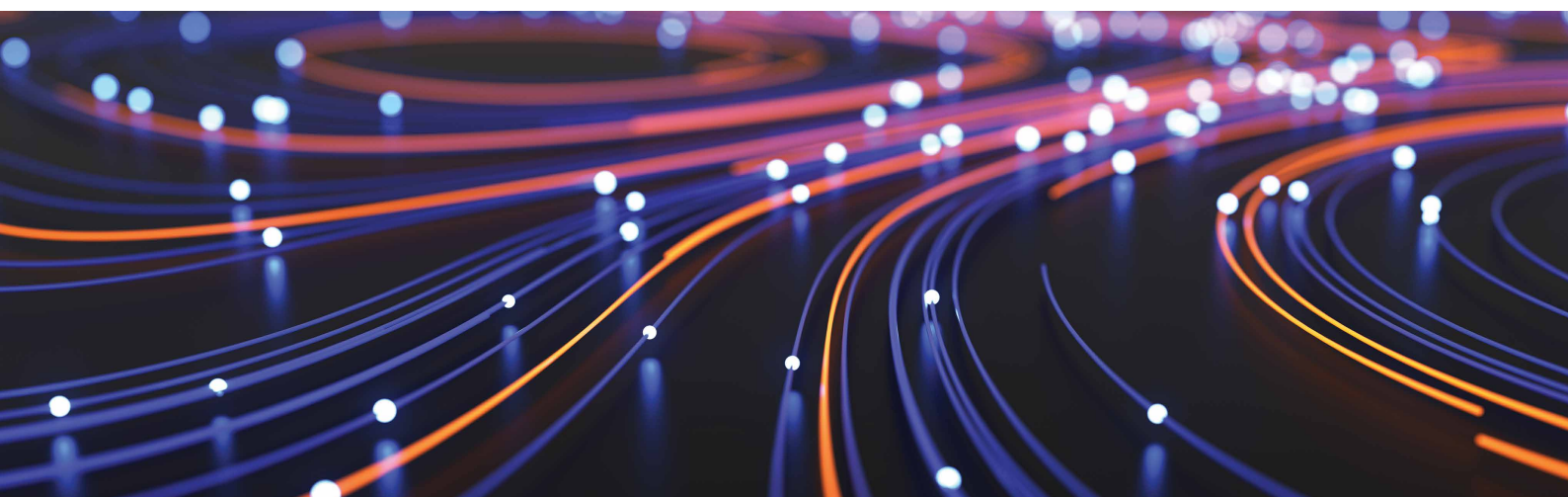
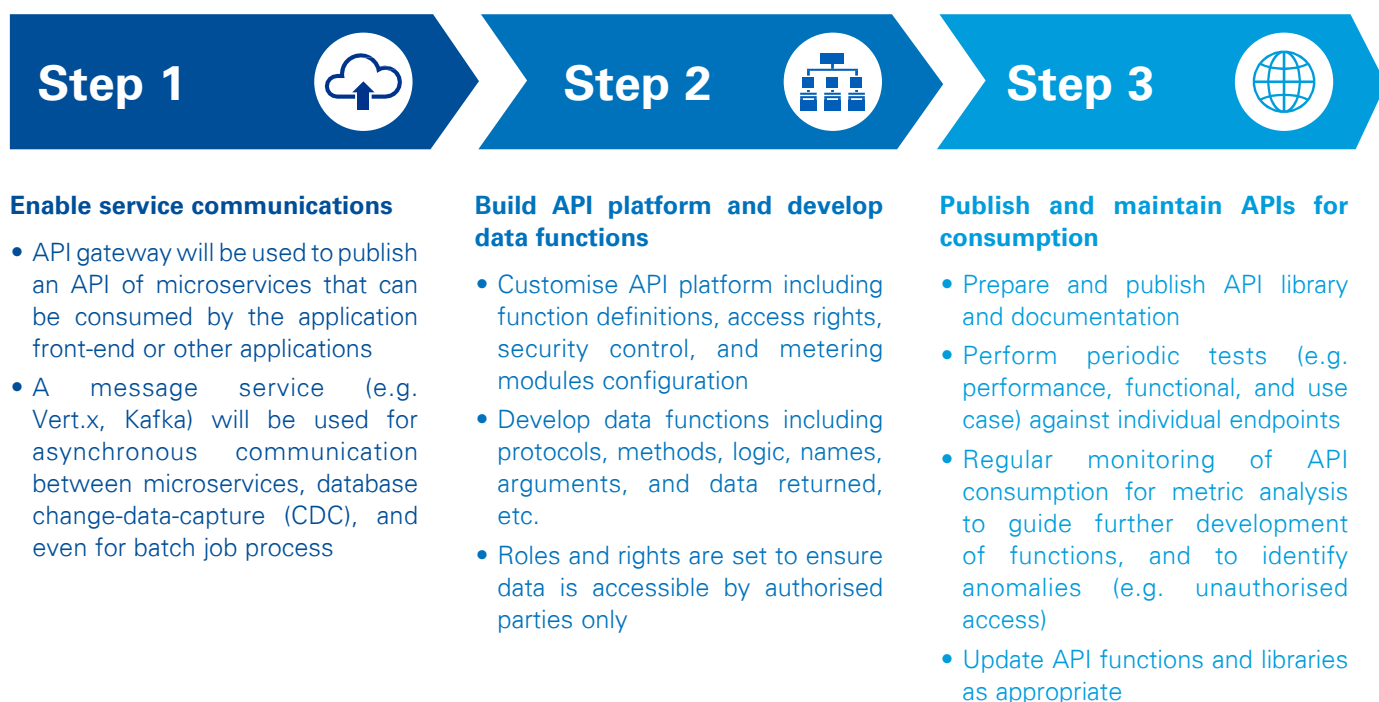


Figure 4: API implementation steps



Source: KPMG

Although APIs help to unwind the complex integration between the legacy system(s) and the Regtech solution, a one-off data migration exercise is still required if the Regtech solution replaces an existing system or application. The misconception that the process is simply moving the data from one place to another could pose a serious threat to banks. Banks should design appropriate plans and establish communication protocols with the vendor to properly manage the migration process. The three main components of the data migration journey are outlined below:

- **Data extraction and preparation** includes extracting data from the old system and ensuring that the data is available and cleansed. Banks need to be mindful of the data requirements for the legacy system and the new platform. This is to avoid any duplicated, missing, or erroneous data in the new system. To understand the data structure disparity between the old and new systems, the bank and the solution provider should prepare a data specification document containing all data requirements. Corrupt or inaccurate data should



be evaluated and either remediated or removed from the dataset. Any data formatting or missing data issues should also be addressed.

- **Data transformation and validation** is the transformation of the relevant and required data to meet the data requirements of the new solution. After the first stage of data extraction, a data transformation process is required to ensure the format is correct and compatible to the new system. Data validation should be performed with exception handling to ensure that data quality is not compromised.
- **Data loading** is the last component of the data migration exercise. Testing should be completed in the new system to ensure the migrated data meets the new requirements. Banks should ensure that they perform testing with the full volume of data in the migration process to cover different scenarios. Sample tests include referential integrity, uniqueness, and null constraints.

3.4 Cloud security

Data security is a continuous process that should be properly managed through robust data governance. Otherwise, it could increase the risk of non-compliance. Cloud-based Regtech solutions should be constantly monitored for any lapses in security, for example through the following areas:

- **Access:** Access controls should be clearly defined and monitored through logging. Any unusual or suspicious behaviour on the application should be checked and verified to meet Cloud security standards. Cloud access keys for different functions/services of Cloud (e.g. programmatic access, management consoles, dashboards, and privileged accounts) should be secured properly, for example, by using multi-factor authentication (MFA) and Virtual Private Network (VPN) encryption.¹⁴ In an instance where staff is working from home and end-user computing devices are used, it is increasingly important to implement appropriate controls to authenticate access to the Cloud-based Regtech.
- **Data protection** is imperative as compromising data security in the Cloud could result in loss of public trust and compliance issue, which consequently requires significant regulatory and IT remediation efforts and costs. Data classification is required to identify the data protection levels to apply the appropriate controls. Any data download via the Regtech solution should be properly monitored and evaluated before authorisation to prevent potential data breach. Appropriate controls should be deployed to prevent data loss, including strong encryption, tokenisation, and logical segregation, which should be assessed on a periodic basis.

¹⁴ Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, Cloud Security Alliance, (July 2017), <https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf>



04 Regtech use cases

Various Cloud-based Regtech solutions have been developed by banks or external vendors. Two use cases and their key learning points are summarised below.

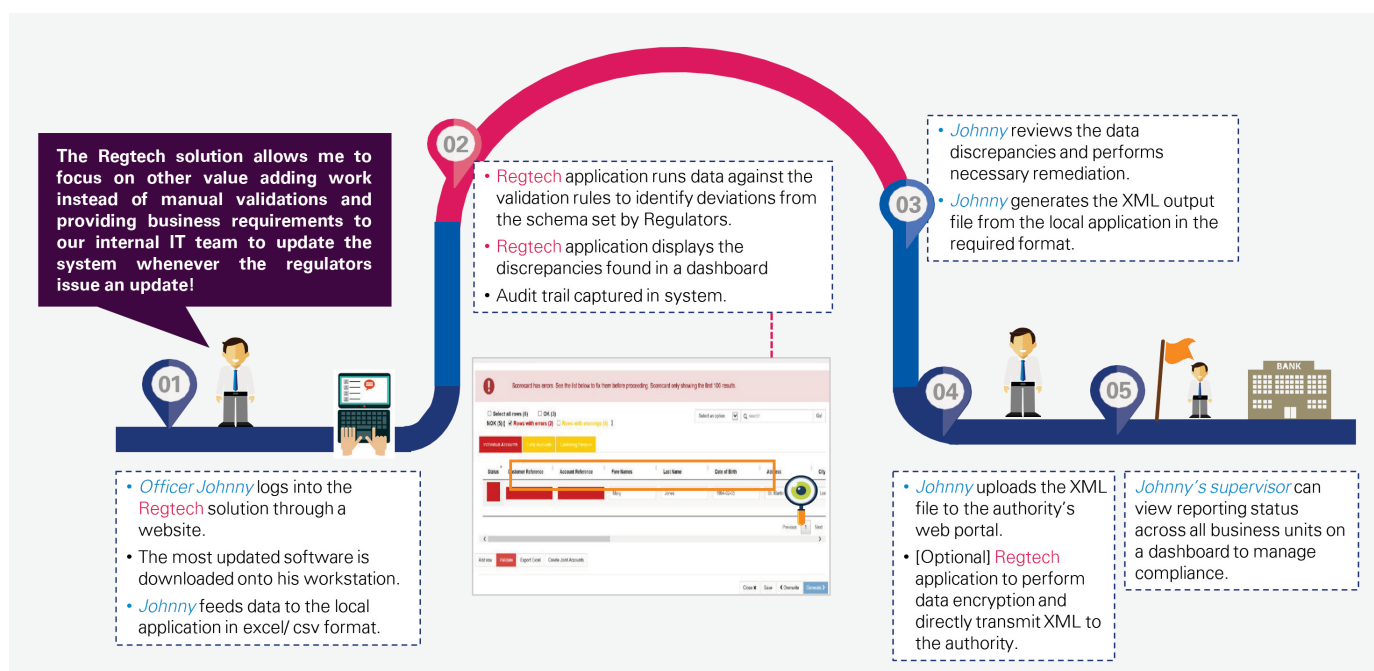
4.1 Use case # 1 – SaaS Regulatory Reporting Tool

Banks are required to report applicable account, customer, or financial details to the regulator on a regular basis

to demonstrate regulatory compliance. To submit its regulatory report, a bank needed to meet the specified data structure and prepared the report according to a pre-defined format. The reporting requirements could be updated by the regulator and the bank needed to comply with the latest requirements.

Cloud-based Regtech solutions can be leveraged to automate the reporting process. The figure below illustrates how the Cloud-based off-the-shelf Regtech solution helped the bank meet its regulatory reporting requirements.

Illustration of use case 1.



By virtue of the Cloud-based Regtech solution, the bank was able to gain the following benefits:

- **Respond to regulatory updates with agility:** Given the schema is subject to frequent updates, it is costly to maintain an internal team of regulatory and technology experts to update the system on an ongoing basis. The Cloud-based Regtech solution features the vendor's offsite support to update the software following the release of new schemas and changes in regulations.
- **Enhanced mobility:** As the Regtech application is Cloud-based, whenever the responsible operators need to produce a report, they can open an internet browser on their workstation and download the most updated application onto their local machine after authentication. As the tool runs on the local workstation and saves output locally, the confidential customer data remains within the organisation. After task completion, the operators log out from the tool and the application is removed from their workstation.
- **Improved user experience:** The Cloud-based Regtech solution is available to users globally with tailored local regulatory compliance requirements. The solution provider is therefore able to make continuous improvements and updates to the application based on consolidated users' feedback. This makes the application more relevant and user-friendly while keeping a constant price.
- **Other additional benefits (not limited to Cloud-based benefits):** Compared to a manual process, there are built-in validation rules in the Regtech solution, thereby enabling the operational staffs to review reportable data and understand the nature of any deviation from the schema in a timely and efficient manner. Secondly, as the regulator requests output in XML data format, the Regtech solution facilitates internal review with a business-friendly version of the XML outputs without requiring staff to understand the schemas set out by the regulator. Further, the Regtech application allows the bank to create user accounts, enables the maker/checker roles assignment and establishes a user-based audit trail, providing appropriate control over data changes and access to outputs.

The Hong Kong-based bank that adopted this Regtech solution is open to Cloud-based technology. The bank has recognised the benefits of Cloud technology and is in the process of making continuous improvements to its established Cloud programme. The business users found

the tool intuitive to use and able to meet the regulatory requirements in a more efficient manner, lessening the reliance on internal IT. The key factors that contributed to the successful implementation are detailed below:

1. Cloud governance framework with risk assessment and intake procedures are already developed by the bank. The business process owner had to follow the established process to seek internal approval to intake the Cloud-based off-the-shelf Regtech solution. The existing intake process was clear, and the management body was able to conduct a risk-based evaluation, which was in contrast to another bank (bank B) where the adoption was unsuccessful. The business owner of bank B was excited about the solution's benefits but cannot find a channel to evaluate the tool as the organisation has yet to on board any Cloud-based solutions.

Key takeaway: Banks need to clearly communicate its Cloud strategy and stance on adopting Cloud-based solutions internally. They also need to establish a clear set of guidelines on the Cloud solution intake process to encourage the business owner to seek and consider innovative Regtech solutions. The intake procedure should involve evaluation and signoff from different parties such as the business, compliance, legal, finance, and IT departments. Together, the committee can form a comprehensive picture of the business benefits and risks of the Regtech solutions.

2. The Regtech solution was flexible in terms of the usage extent of the Cloud technology. The Regtech solution delivers the latest software via Cloud technology, and the latest programme is always available for users to download. The Regtech solution allowed the bank to generate the report using a local machine, with the option to either upload the file to the authority by the bank's officer (so confidential customer data remains secure within the bank), or submit data directly to the authority by the Regtech solution where the bank needs to evaluate the data encryption capabilities.

Key takeaway: Regtech solution providers should understand that customer data is one of the bank's key assets. Banks are protective of the customer data and concerned about data privacy and security risks around Cloud-based applications. To aid successful evaluation and adoption, Regtech providers will need to be ready to prove that the Cloud-based solution does not increase data security risks, and that it fits into a bank's overall security architecture.



3. The Cloud-based Regtech solution was built in conjunction with local risk management and regulatory compliance subject matter experts within the bank. The review by experts ensured that the Regtech solution met the authority's reporting requirements, and continuously complied via updates delivered over the Cloud. Being an off-the-shelf application, configuration and setup of user profiles took around one day, then it was available for download and use.

Key takeaway: With the option to provide a one-way delivery of data with no data to be uploaded to the Cloud, the solution is flexible enough to meet the evaluation criteria of different banks. **Regtech solution providers** should understand that technology will not be the sole contributing factor for banks to adopt a Regtech solution. Local regulatory expertise is required to make the tool relevant and to assist banks in meeting regulatory requirements. Cloud technology enables the Regtech solution providers to provide offsite and timely technical support to ease the implementation process.

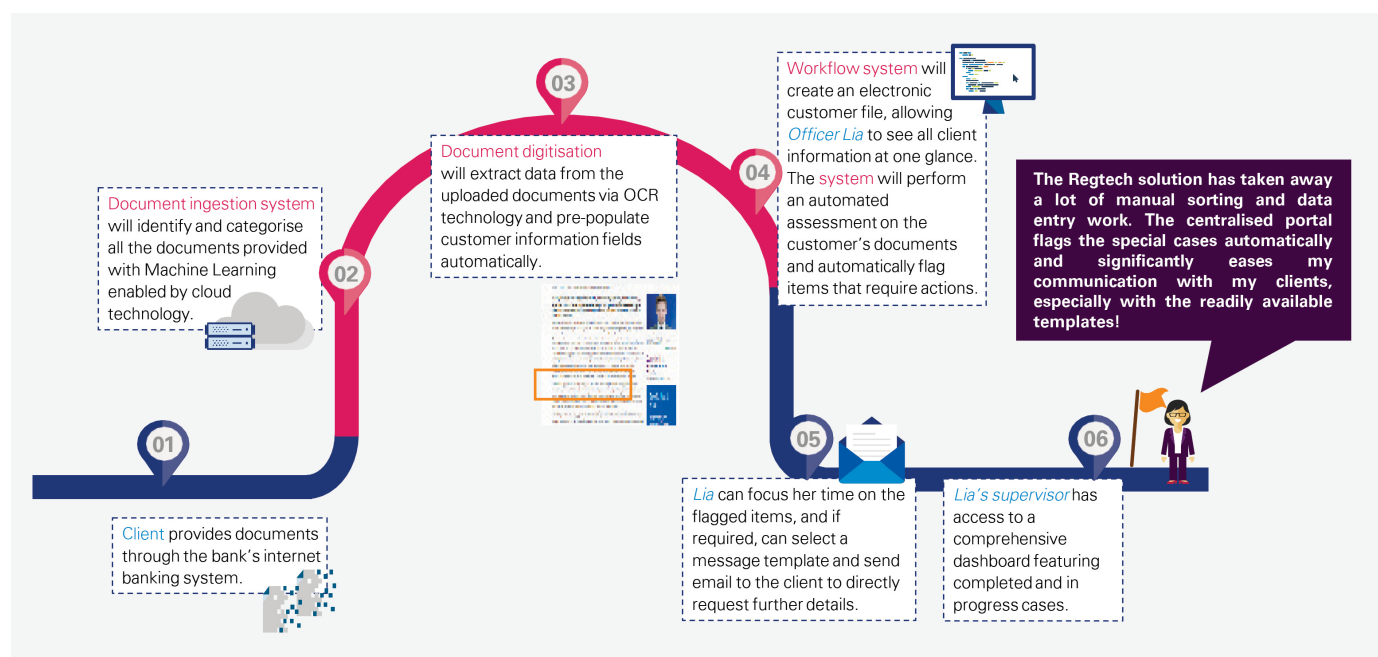
4.2 Use case # 2 – Cloud-enabled Customer Document Review and Management platform

Evaluation of customer documents is required across multiple areas of banks to support compliance and risk management requirements. For example, verification of customer documents for credit assessment or customer due diligence that occurs during onboarding and continues throughout the banking relationship. Banks are required to complete more comprehensive customer due diligence processes due to increased international efforts to combat illegal activities such as tax evasion.¹⁵ These processes, which are resource intensive, are important in managing the overall business risk to banks.

Cloud-based Regtech solutions have the potential to transform these processes from what may have been perceived as a compliance tick-box exercise, to the holistic management of risks evidenced by a robust audit trail. Cloud-based Regtech solutions can also enhance customer experience by leveraging existing information that customers have previously submitted and enabling remote customer document submissions by leveraging emerging technologies like Optical Character Recognition (OCR).

The Cloud-based, Artificial Intelligence-enabled client information management platform depicted in the illustration allowed a bank to automate the assessment and classification of unstructured documents for each customer, and along with a built-in workflow, was able to significantly increase efficiency, moving from a manual process averaging 11 hours per case to 5 hours per case.

Illustration of use case 2.



The bank adopted the Cloud-based Regtech platform solution as it wanted to build a scalable solution that could meet business demands and enhance customer experience. The bank chose a Hong Kong Cloud-based platform with all data and back-end systems hosted locally. The key success factors that contributed to the successful implementation are detailed below:

1. The full solution was of a very large scale and involved material offshoring of client due diligence operations and the implementation of a Cloud-based platform. The bank had established an enterprise-wide Cloud governance framework and a governance committee which assisted with the intake process. It took around six months for the bank to obtain necessary internal and regulatory approvals. In particular, the bank had to perform the following internal and external risk assessments:

¹⁵ Account Opening and Maintenance, Hong Kong Monetary Authority, <https://www.hkma.gov.hk/eng/smart-consumers/account-opening/>

- Internal IT review of the platform solution's Cloud security and controls, architecture and data transfer processes
- Penetration test on the Cloud-based Platform solution to uncover any vulnerabilities or points of ingress
- Internal legal and compliance reviews on the Cloud environment and data hosting and transfer risks
- Internal review on the Cloud-based platform solution vendor in terms of operational, legal, and reputational risks
- Independent assessment on the HKMA regulatory requirements (e.g. business continuity plan, contract, and Service-level Agreement).
- Risk assessment on Cloud technology & material outsourcing project

Key takeaway: Banks should establish a framework that outlines all the necessary reviews required to fully evaluate a solution. Banks should also note that the risk evaluation and approval process for Cloud solutions may take a substantial amount of time, and should therefore budget time and resources to evaluate the large Cloud-based platform solutions ahead of design and implementation.

2. The bank was working with on-premises legacy systems. The Cloud-based platform offered an API-based integration framework, which allowed all approved applications to be integrated in real-time as compared to historical batch processing jobs. The Regtech solution provider built the platform with best practice architecture, utilising a low code platform to increase the solution's configurability, and adopting microservices to allow for parallel development and change delivery. The platform implementation followed a strict project management framework and contained activities such as planning, data migration, system integration, platform configuration, testing, preparing for operational readiness, and go-live support.

Key takeaway: Banks are required to form a dedicated project team to deliver the customised platform together with the vendor. In-house enterprise architects and cybersecurity architects experienced with Cloud-based integration and implementation will be the key during solution evaluation, design, and implementation stages. It is imperative that banks are involved throughout the platform design and implementation stages, and work closely with the vendor to deliver a solution that is fit for purpose. In addition, the in-house project team is required to provide input and signoff on the user journey, functional and non-functional requirements, and support system integration, compliance and risk reviews, testing, organisational change, and operation readiness.

A

Appendix

A.1 Acknowledgements

KPMG co-authors and subject matter expert contributors: Paul McSheaffrey, Stanley Sum, James O’Callaghan, Marcos Chow, Brian Cheung, Angela Zhang, Edward Choi, Amos Lam, Alvin Wong, Kelly, Albert Tan, editor Kanishk Verghese

A.2 Relevant regulatory requirements and/or guidance

Name	Link
HKMA Supervisory Policy Manual – Outsourcing (SA-2)	https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/SA-2.pdf
HKMA Supervisory Policy Manual – Risk Management of E-Banking – Supervisory Policy Manual (TM-E-1)	https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-E-1.pdf
HKMA Supervisory Policy Manual – General Principles for Technology Risk Management (TM-G-1)	https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-1.pdf
HKMA Circular – “Customer Data Protection”	https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2014/20141014e1.pdf
Office of the Privacy Commissioner for Personal Data, Hong Kong – Cloud Computing	https://www.pcpd.org.hk/english/resources_centre/publications/files/IL_cloud_e.pdf
Office of the Privacy Commissioner for Personal Data, Hong Kong – Guidance on Personal Data Protection in Cross-border Data Transfer	https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf