Regtech Adoption Practice Guide

Issue #7: Third-Party Monitoring and Risk Management

July 2022

HONG KONG MONETARY AUTHORITY
香港金融管理局

KPMG

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

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 identified 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, and the Fintech Supervisory Chatroom. Ultimately, the Guides should enhance the sharing of experience related to Regtech implementation in the industry, which will help to further drive Regtech adoption in Hong Kong.

This seventh Guide of the series focuses on Third-Party Monitoring and Risk Management (TPRM) and related Regtech solutions. There has been incredible growth in

[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

the reliance of businesses on third-parties in recent years, from third-party vendors that a business works with across its value chain to dependence on a third-party's solution. In an environment that is constantly developing, new technologies are introduced and, with that, also new risks. Investing in TPRM would ensure that the risk associated with vendors is reduced, allowing a business to keep functioning efficiently in a more secure environment.

1.2 Purpose

The purpose of this Guide is to provide an overview of the Regtech solutions used in Third-Party Monitoring and Risk Management, outline the common challenges observed during implementation, and share experience on how others have addressed the challenges to successfully adopting Regtech solutions in their organisations. This Guide follows the outline below:

1 **Explain how Regtech solutions can be used to support Third-Party Monitoring and Risk Management**

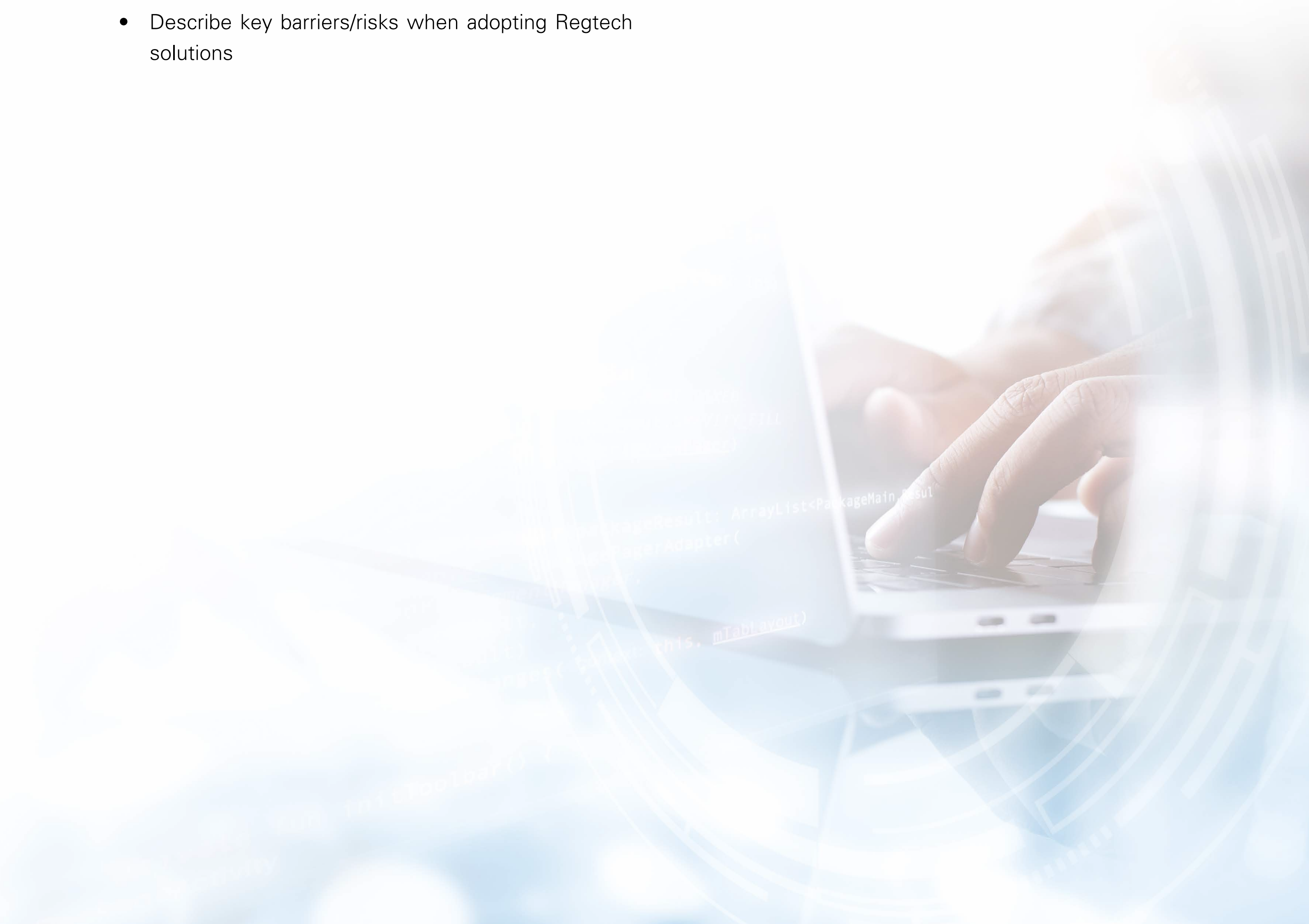
- Illustrate the benefits of leveraging Regtech solutions
- Describe key barriers/risks when adopting Regtech solutions

2 **Provide practical implementation guidance to banks on the adoption of Regtech solutions for Third-Party Monitoring and Risk Management**

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

3 **Share use cases on the adoption of Regtech solutions for Third-Party Monitoring and Risk Management**

- 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



02 Third-Party Monitoring and Risk Management

2.1 Key challenges/ developments

Growing complexity in the vendor ecosystem

Third-party collaboration is deeply ingrained in banking operations, from traditional vendors such as technology providers, custodians and clearing agents to data providers, cloud providers, and other partners who are crucial for new business acquisition. The breadth of third-party services and solutions brings increased complexity for banks who need to manage the risk associated with third-party use.

There are a few key aspects that banks must consider when it comes to assessing third-party services.

Firstly, banks must have a precise inventory of the third-parties that they work with – categorised by the nature of the relationship, e.g. outsourcing or non-outsourcing relationships, and the criticality of the relationship, i.e. its importance within the bank's value chain. Market insight indicates that banks often find it challenging to maintain and consolidate a central inventory of all third-parties.

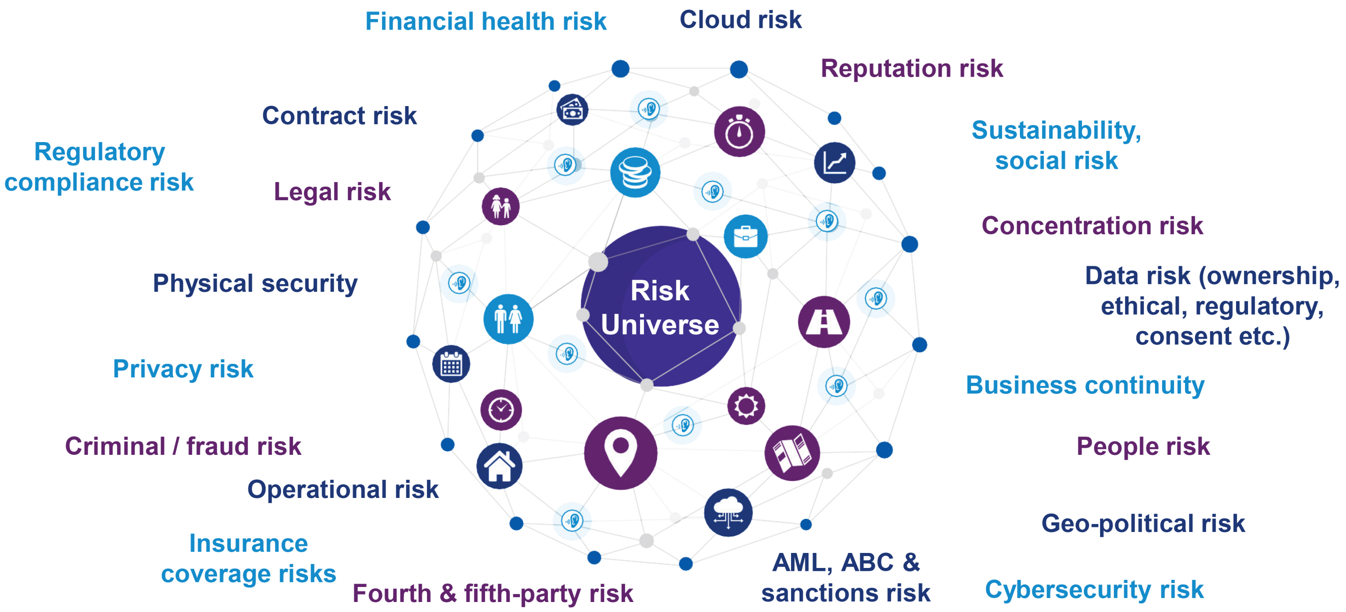
Figure 1: Third-party landscape

EXAMPLE THIRD-PARTY LANDSCAPE			
Cloud service providers	Fintechs & e-comm merchants	Affiliates	Industry utility / API providers
Analytics services	Channel partners	Vendors (operations and IT)	Virtual customer care centres (Voice, Email, Chat, Chat-bot, AI)
Data firms	Payment processing partners	Records management	Merchants
Consultants	Marketing / advertising agencies	Debt collectors & credit services providers	Storage & backup service providers
Facilities services providers	ATM management	Print and mailing services	Loyalty partners
Stock exchange	Open banking intermediaries & wallets	Joint ventures	Fund administrators

Secondly, banks must consider the risk profile of the third-parties. As Figure 2 shows, there is a wide spectrum of risks that should be considered during the third-party assessment process. Banks must understand the nature and criticality of the third-party relationship to ensure the right considerations are applied in their inherent risk assessment process.

In particular, risk categories that have historically not been sufficiently considered, such as sustainability risk or suppliers' sub-contracting risks, need to be given due consideration. Assessment of critical supplier's sub-contracting risks was a notable weakness for many banks during the pandemic when third-party outages or service delivery problems were frequently caused by a third-party's reliance on other service providers. Without the right TPRM processes, these risks would be difficult to identify and manage effectively.

Figure 2: Risk universe

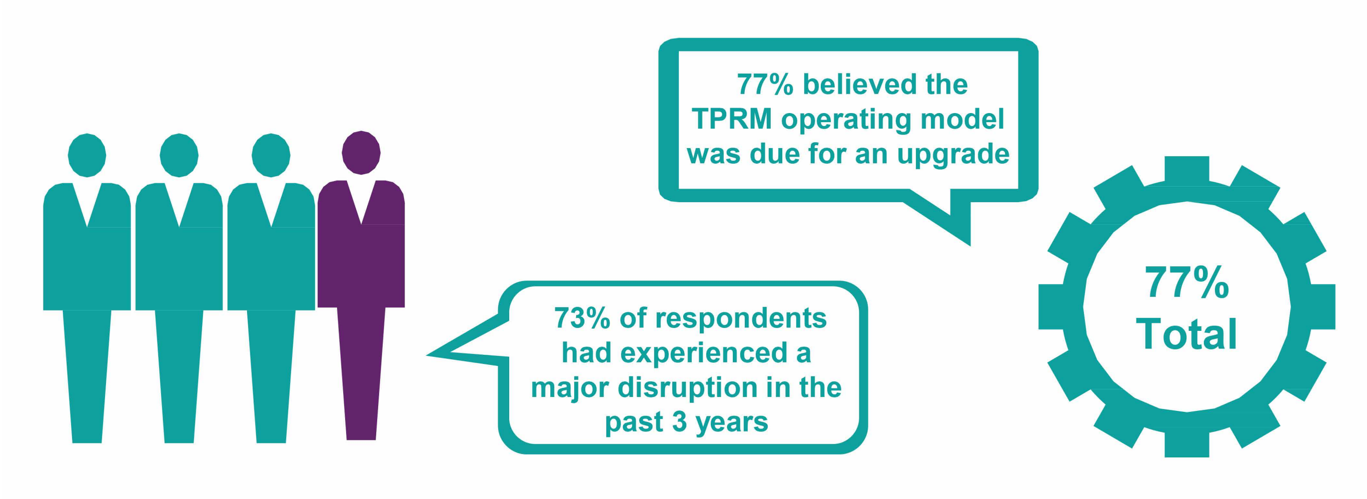


TPRM operating models lack robustness

Banks often need to work with fragmented technology platforms across different parts of the TPRM lifecycle. This, coupled with challenges associated with managing the ever-expanding third-party relationships and the wider risk universe outlined in Figure 2, is prompting organisations to reassess and enhance their operating models.

In KPMG's Global TPRM Outlook 2022 Survey, 77% of banks believe that their TPRM operating model is due for an upgrade. In addition, many banks regularly experience third-party-related incidents that need to be managed and prevented. In the same survey, 73% of respondents had experienced a major disruption in connection with a third-party in the past three years.

Figure 3: Findings from KPMG's TPRM Outlook 2022 Survey


77% believed the TPRM operating model was due for an upgrade
73% of respondents had experienced a major disruption in the past 3 years
77% Total

Regulatory Requirements

The TPRM operating model is not a standalone risk discipline, and it is interwoven with many other regulatory and risk disciplines across the bank, such as climate risk management, recovery & resolution planning, and operational resilience, to name a few.

The HKMA requires banks to have a clear view of critical business processes and services and likewise identify the role that third-parties play in these critical areas[2]. The approach to risk assessment across various regulatory and governance priorities should be applied consistently and adhered to regulatory requirements.

Technology is underutilised or not consistently applied across banks

Many banks now have technology enabled TPRM solutions in place, however, 59% of respondents in KPMG International's TPRM Outlook 2022 Survey cited their frustration with the lack of visibility that their technology gave them on third-party risk across the TPRM lifecycle. It is important that banks are aware of the most common pitfalls of technology solution implementations that include, but may not be limited to:

- Lack of automation or limitations in functionality
- Lack of data-driven insight, in particular, the ability to support dashboard reporting
- Lack of alignment and integration with TPRM operating model and enterprise-wide risk programmes

[2] HKMA Supervisory Policy Manual: OR-2 Operational Resilience https://www.hkma.gov.hk/media/eng/doc/key-functions/ banking-stability/supervisory-policy-manual/OR-2.pdf

2.2 Key considerations when adopting Third-Party Monitoring and Risk Management Regtech solutions

There are a number of aspects that banks should consider to ensure the successful adoption of Regtech in TPRM:

Data quality

Many banks have experienced an expectation gap when implementing TPRM Regtech solutions because the fundamental issues with data quality have not been addressed. Good quality data is needed at the right points to help banks understand, assess and monitor third-parties. Data clean-up and improvement initiatives may be required to maximise the value of the Regtech solution. Key considerations should be:

- **Data availability:** The right data at the right granularity feeding the Regtech solution at the right time to allow a timely and effective process to be run.
- **Data integrity:** The data need to be sufficiently robust to represent a 'single version of the truth' or 'golden source' that can be relied upon.

Enterprise-wide approach

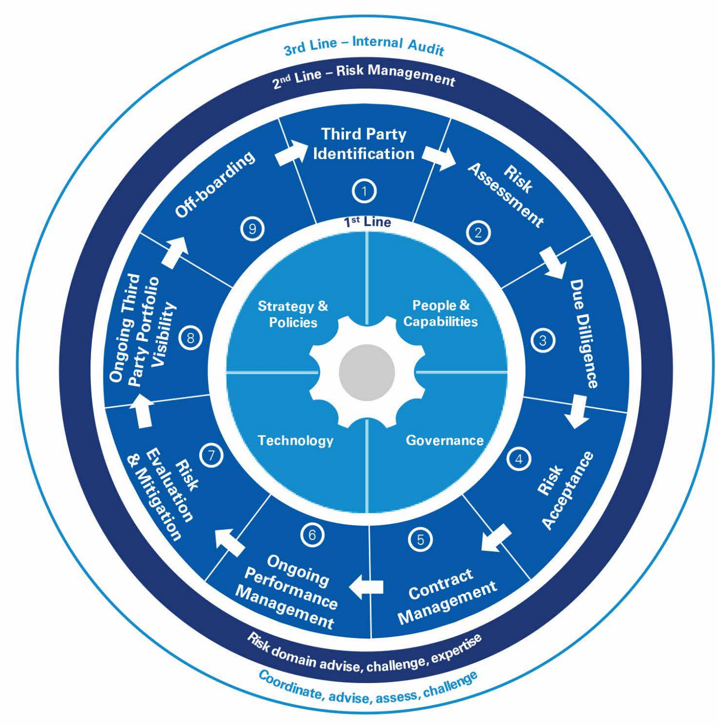
As mentioned previously, third-parties are used across the bank value chain and are often highly integrated into a bank's ecosystem. As such, the operating model (governance, people and process) surrounding the Regtech application should also be enterprise-wide to allow the process and tool to be effective. Banks should consider the following aspects in the design and selection of their Regtech solution(s):

- **Functionality:** The target solution must be capable of delivering the emerging functional requirements whilst remaining aligned with the bank's broader technology strategy.
- **Architectural design:** Understanding how the different systems interface with one another is essential to delivering enterprise-wide connectivity.
- **Data model:** Having a defined data model, including internal and external data sources, is critical to an enterprise-wide solution that uses multiple data sources.
- **Integration:** The solution must be able to integrate with other relevant processes and systems (e.g. operational resilience, procurement, contract lifecycle management, and vendor performance systems).
- **Alignment:** Understanding the implication of other system initiatives, projects, or remediation efforts is critical to defining a suitable implementation path for the solution.

Operating model

The operating model is a key consideration for any technology implementation. Banks need to consider how TPRM integrates across different functions, e.g. procurement, legal, finance, audit, and across governance requirements such as outsourcing or operational resilience. Getting alignment across the whole organisation can be challenging as many stakeholders are involved. Thus, roles and responsibilities need to be constructed to reflect a TPRM-specific mandate in each function, and the service delivery model should be examined to show how TPRM integrates into other bank processes. The operating model must be drawn up in a way that covers all three lines of defence, as shown in the sample TPRM framework in Figure 4.

Figure 4: Sample TPRM framework


3rd Line – Internal Audit
2nd Line – Risk Management
Third Party Identification
1
Risk Assessment
2
Due Diligence
3
Risk Acceptance
4
Contract Management
5
Ongoing Performance Management
6
Risk Evaluation & Mitigation
7
Ongoing Third Party Portfolio Visibility
8
Off-boarding
9
1st Line
Strategy & Policies
People & Capabilities
Technology
Governance
Risk domain advise, challenge, expertise
Coordinate, advise, assess, challenge

TPRM-specific activities should be reviewed, and where necessary new processes must be implemented to ensure that a comprehensive TPRM operating model is in place. This should cover processes such as:

- Business criticality and risk assessment
- Inherent and residual risk calculation
- Dynamic risk monitoring
- Escalation, reporting and feedback channels
- Comprehensive due diligence

Dynamic third-party risk monitoring across the TPRM lifecycle

The TPRM operating model needs to be dynamic as a third-party's risk profile can change on an ongoing basis. As such, the risk profile of the third-party must be continuously monitored after initial onboarding, and risk assessment must be repeated when necessary. Banks must know how changes in their own set-up, as well as changes at the third-party, impact their own risk profile and whether additional action needs to be taken.

Leveraging a technology solution that enables dynamic third-party risk monitoring is critical from a risk management perspective. It allows organisations to easily look through supplier relationships to identify suppliers' sub-contracting risks and stay on top of changes as they occur which facilitates monitoring across a wider risk universe.

To illustrate these benefits, Artificial Intelligence (AI)-enabled risk modelling engines can provide the following benefits to banks:

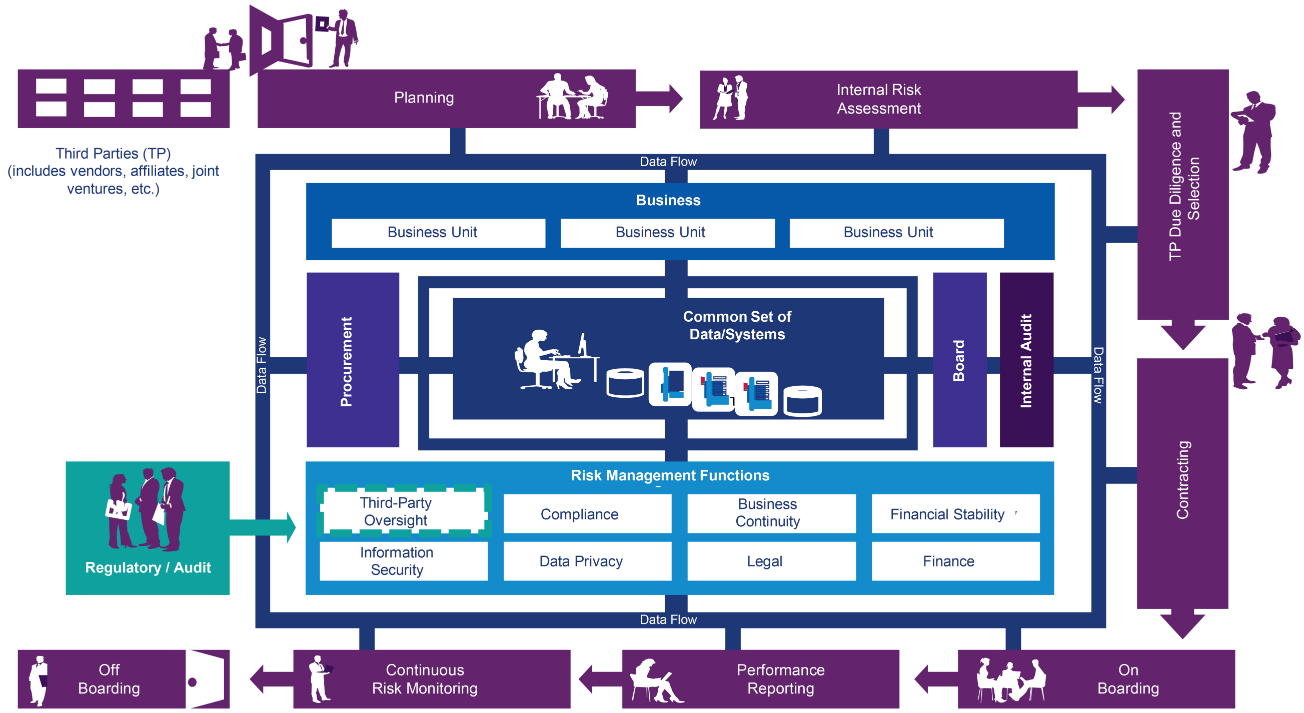
- Big data-driven analysis can help to identify hidden patterns and correlations to provide more accurate criticality calculation of the third-party.

- AI is able to detect third-party vulnerabilities, such as global risk exposure across third-parties, where the highest level of risk is likely to occur, and which specific third-parties are the most vulnerable.

- End-to-end scenario modelling can identify which particular areas of the third-party are most vulnerable and estimate the value that could be lost or impacted if incidents do arise.

As highlighted previously, TPRM is a lifecycle-based process that traverses the entire enterprise. Technology solutions can tie all the lifecycle elements together in a way that a manual process can never do.

Figure 5: TPRM lifecycle



Inherent risk assessment and due diligence automation

The cornerstone of a technology-enabled TPRM infrastructure is the traceability of data. It is crucial to have a 'golden source' of data and a defined data model for profiling third-parties for due diligence, monitoring, risk assessment, and other issues. For global institutions, cross-border data analysis is critical, particularly for material global relationships.

Having current and high quality-data in the third-party inventory improves the accuracy of risk assessments as it provides a clear view of material third-party relationships. Automation of the assessment process, including tiering assessments, due diligence checks, and vendor assessments, reduces the need for manual intervention except when judgement is required. Technology can also flag emerging areas of concern more timely than a manual process.

Overall, considering the complexities outlined earlier, there are clearly compliance and risk management benefits for banks that apply technology across the TPRM process, not to mention the reduction of process inefficiency.

Real-time monitoring

TPRM Regtech solutions can offer real-time monitoring and service disruption alerts based on internal and external data sources before they occur, allowing banks to proactively manage their risk exposures. Insights and analysis also give the ability to track, report and predict incidents. This can then be used to generate key performance and risk indicators (KPIs/KRIs) at the service level that can be fed upward to senior management and the board in the form of Management Information (MI) reporting.

Lastly, the use of TPRM Regtech solutions provides a demonstration and audit trail of good governance to address regulatory concerns across the globe.

Enterprise integration

Designing an integrated operating model, including supporting IT Architecture, is the glue that holds everything together. Workflow automation and centralised data stores allow data sources from across the TPRM programme to be hosted in one location and distributed upstream to other feeds, thus ensuring connectivity and consistency.

03 Implementation guidance

TPRM Regtech solutions can provide many benefits. However, careful planning must be carried out for the implementation of such a business-critical solution to avoid any negative impacts. As a pre-requisite for Regtech adoption, banks should have a clear understanding of their operating model and the capabilities of their people. There needs to be a clear articulation of the TPRM mandate across different departments and functions.

3.1 Strategy and operating model

TPRM strategy and operating model should be reviewed before Regtech solution implementation to ensure governance, processes, policies and controls are clearly defined and consistently implemented across the organisation.

Subsequent to the review, enhancements should be made to address any findings to optimise the operating model. The review and enhancement process is critical in maximising the value of technology investment. Banks that do not have an existing operating model in place should first focus on developing a fit-for-purpose TPRM approach and operating model.

As noted previously in this guide, TPRM has multiple touchpoints across the banks and covers a wide range of risk disciplines (e.g. outsourcing, operational resilience, technology risk, sustainability or continuity). As such, it is important to align the operating model to agree on the desired outcome of a Regtech investment collectively with all stakeholders.

3.2 People and capabilities

Understanding whether there is capacity and capability within TPRM to support the Regtech implementation is critical. Banks should evaluate skill gaps and identify user training required to ensure the solution can be utilised effectively. To manage this proactively, banks need to develop a coherent change management strategy and implementation roadmap driven by TPRM.

Deploying a solution without adequate training and involvement of the TPRM team may increase the risk that the solution does not fully meet expectations and business requirements. To mitigate this risk, TPRM teams should be involved in defining functional requirements and solution design.

3.3 Governance and organisation

Within banks, the TPRM programme needs to straddle both the first and second lines of defence to be effective.

Regardless of the types of the operation model and how the ownership of TPRM processes and activities are assigned, there must be a clear articulation of the TPRM mandate and roles and responsibilities across different departments and functions. Successful implementation of an enterprise-wide solution would require all relevant departments (e.g. business, procurement, finance, operation risk or legal) to work in tandem and be involved from day one of the planning phases.

3.4 Technology and data

Data collection

The availability and integrity assessment of TPRM-related data should be a bottom-up approach. Starting from the data collection point, the supplier onboarding questionnaire needs to include a host of data inputs that will form the third-party profile, such as information on the scope of service of the third-party, compliance considerations, cloud hosting, risk assessment result, threat management, business resiliency, operations management, sustainability features, and asset and information management to name a few.

It is also critical that the third-party reference data then need to be re-assessed and updated periodically or when a triggering event has been identified (e.g. a third-party gets into financial difficulties or is embroiled in a scandal).

Functionality

When assessing the suitability of a solution, there is a set of standard TPRM solution capabilities that should be considered, which include:

- Storing and maintaining a comprehensive record of third-party profile data

- Managing end-to-end workflow for on/off-boarding, contract compliance review, regular performance monitoring, and periodic re-evaluation of the third-party risk profile

- Providing auto-alerts for risk trigger events based on internal/external data or pre-defined red flag indicators

- Ability to capture team judgment calls on risk acceptance and automatically calculate residual risk

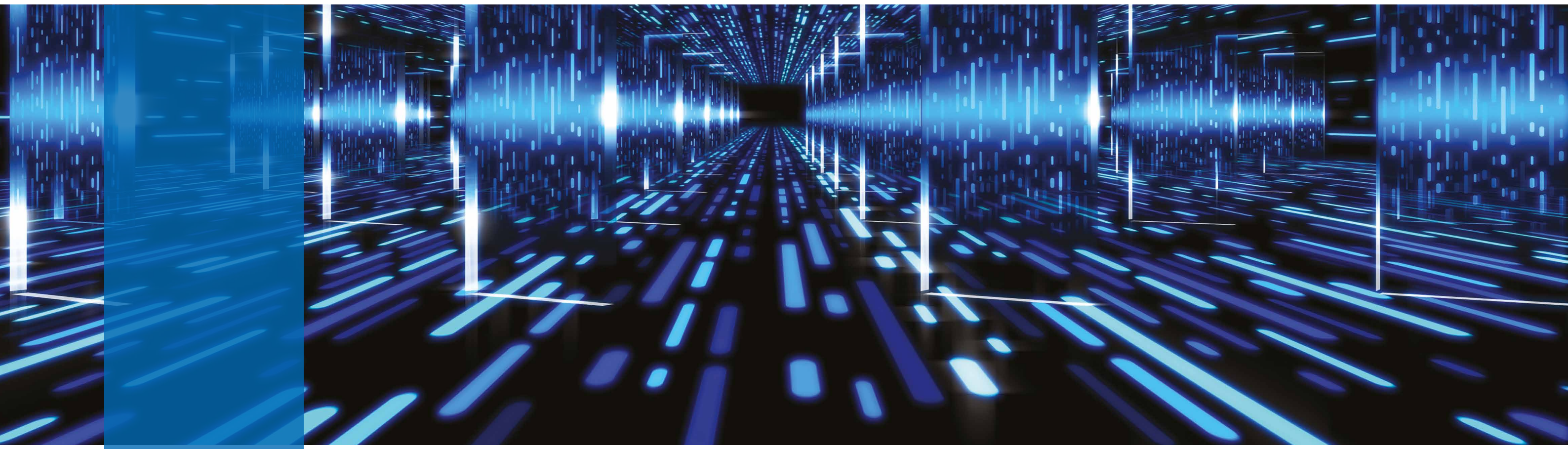
- Providing an interface for the third-party to interact/share information with the bank, e.g. to submit supporting documents to facilitate the initial or ongoing due diligence process

A solution with the above capabilities will cover all aspects of the TPRM lifecycle, from third-party identification to off-boarding. The automation of key functions such as auto alerts significantly reduces manual work and helps the bank keep a current view of the risk profile of the third-parties.

In-house vs off-the-shelf

Another key decision to make is “buy” or “develop”, from development/implementation time, adequacy of skillset, monetary cost (upfront/hidden/ongoing), infrastructure compatibility, functionality to performance. There is a long list of consideration points.

Ultimately, the decision should link back to the mission and objectives of the TPRM programme, the bank’s ability to develop such a solution by itself, and the strength of the in-house team. The bank should also adequately factor in a cost-benefit analysis and risk-based approach when implementing TPRM Regtech solution.



04 Regtech use cases

4.1 Use Case #1 – Cloud-based TPRM platform

4.1.1 Challenge

A leading global bank with significant cross-border operations had historically struggled to maintain a holistic view of its bank-wide critical third-parties due to its complex network of third-party collaborations and lack of transparency over cross-border operations.

As the bank's third-party vendor network continued to grow, it was essential to synthesise large volumes of data in order to perform materiality assessments on third-parties. For example, some large technology suppliers were used by the bank in almost all locations, but the bank had no consolidated visibility of the overall work scope and performance of these suppliers.

Additionally, there were other challenges:

- Lack of consistent TPRM operating model across different functions and locations
- Lack of procurement platform feature to automate risk assessment and capture various assessment results into one single repository
- Lack of system integration between procurement platform and contract lifecycle management tools, governance, risk and compliance tools or incident management solutions

Facing the challenges, the bank wanted to explore opportunities to implement an enterprise-wide platform that would operate across the TPRM lifecycle – capturing all third-party information into a single repository that allowed for ongoing criticality and risk assessment, monitoring, reporting and integration with other banking solutions.

4.1.2 Solution

In order to address the challenges laid out above, the bank opted for a highly customisable and scalable cloud-based solution. The solution gave the bank the ability to maintain a centralised and up-to-date set of third-party information, enhanced transparency and accessibility of third-party information across the bank and automated end-to-end workflow across the TRPM lifecycle to create efficiency and reduce human errors.

4.1.3 Key success factors

Cloud-based solution: Leveraging a dedicated cloud-based solution was instrumental to the success of the implementation. The scalability and functionality that the solution offered enabled the bank to manage the increasing volume of outsourcing relationships and risk assessments with minimum manual effort.

TPRM framework review: Analysing the TPRM framework and the TPRM lifecycle from onboarding through to off-boarding gave the bank clarity on which relevant systems needed to be integrated with the TPRM solution. Furthermore, the bank was able to establish which functions in the bank would be responsible for owning which parts of the implementation and the future state processes. In particular, the critical roles of procurement, the risk function and the business teams were clarified in third-party engagements.

Data quality and availability assessment: Prior to implementation, the bank reviewed the data availability and quality within the TPRM lifecycle and identified poor data quality issues due to lack of connectivity and synchronisation between contract management and procurement system, e.g. inconsistent supplier naming, lack of unique supplier identifier, missing data points in the third-party reference data.

The selected cloud-based solution allowed the bank to automate the workflow so that the third-party inventory tool could be connected to the contract management and procurement systems to allow centralisation and synchronisation of third-party information – enabling the bank to have a 'golden source' of data.

4.2 Use case #2 - Automated residual risk assessment

4.2.1 Challenge

A large international bank with operations in Hong Kong had always experienced efficiency and effectiveness issues with its manual-based third-party due diligence and risk assessment processes.

Besides it being a time-consuming process, with rigid risk assessment questionnaires, the bank was also finding it difficult to identify trigger events that required a re-evaluation of a particular third-party's risk profile and risk assessment. e.g. negative news and supply chain challenges that could require a re-evaluation of a particular third-party's risk profile.

The pandemic and its impact on third-parties (e.g. business closures and high absentee levels) have especially highlighted the need for such an early warning to inform the bank when a third-party's risk profile changes.

Furthermore, results of different sets of risk assessment questionnaires were maintained by different business units within the bank, without a centralised system and capability to conduct data analysis and reporting.

4.2.2 Solution

The bank was able to identify and implement an end-to-end Regtech solution that addressed the challenges with a number of features, including:

Dynamic risk assessment

The solution scanned external data feeds such as news, and social media feeds, supply chain indicators and applied machine learning and AI to match potential external threats or risk indicators to the bank's third-party universe and alerted the bank when a third-party re-evaluation was required.

Continuous monitoring and visualisation

The dashboard with the heat-map function provided a view of hot risk zones/regions based on each risk type (across the different specified risk lenses), which allowed users to analyse potential regions that were risk hot spots and required focus.

4.2.3 Key success factors

Clearly mapping all the roles and responsibilities: In this instance, the bank's TPRM team sat in the second line of defence and did not actually complete the assessments. The frontline business unit or corporate function looking to engage a third-party was responsible for owning the relationship with the third-party, but also completing the residual risk assessment. The new tool allowed the first line and second line both to discharge their duty around third-party risk monitoring and oversight within the same platform. All parties of the bank worked together to ensure a comprehensive approach was identified and factored into the business requirements.

Utilisation of the data for ongoing monitoring: As mentioned above, data availability for the bank was a major pain point in achieving transparency across the third-party ecosystem. The programme was accompanied by a major data cleansing exercise covering activities such as archiving third-parties not used frequently or aligning identities globally so that third-parties within the same legal entity group could be linked. The amount of work should not be underestimated, but the results were very positive. The bank was in a much better position to see and monitor global and local critical third-parties and bring relevant management information to their various risk governance forums.

05 Conclusion

Any Regtech third-party monitoring tool implementation is a highly complex initiative to deliver. A thorough analysis must be performed to understand the cost-benefit of implementation. Likewise, there must be strong support from the business to make an implementation successful. Accompanying this, there should be a well-documented implementation roadmap and change management strategy. At the same time, we can see that proactive TPRM is complex and spans the entire organisation. It is impossible to run such activity well without integrated technology support.

In this respect, a comparison can be drawn to client onboarding – which is a similarly complex lifecycle process (arguably less dispersed across the whole enterprise) and has received significant amounts of investment across all banks, including investment in Regtech solutions. This has resulted in a significant reduction in onboarding time and enhanced risk management for banks. The return on investment for client onboarding teams has been transformational, and TPRM would be no different.

Banks are now dealing with an increasingly complex array of third-parties. Current manual processes are not future-proof solutions for analysing the large volumes of data and risk considerations needed to proactively manage third-party risk. Deploying Regtech solutions is a viable measure for banks to build long-term, scalable and sustainable TPRM programmes.

A Appendix

A.1 Acknowledgements

KPMG co-authors and subject matter expert contributors: Paul McSheaffrey, James O'Callaghan, Isabel Zisselsberger, Stanley Sum, editor Philip Wiggenraad

A.2 Relevant regulatory requirements and/or guidance

Name	Link
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
HKMA Supervisory Policy Manual – Operational Risk Management (OR-1)	https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-1.pdf
HKMA Supervisory Manual - Operational Resilience (OR-2)	https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/OR-2.pdf
HKMA Supervisory Manual – Climate Risk Management (GS-1)	https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/GS-1.pdf
HKMA Supervisory Manual – Recovery Planning (RE-1)	https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/RE-1.pdf
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 – 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 Supervisory Policy Manual – Business Continuity Planning (TM-G-2)	https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/supervisory-policy-manual/TM-G-2.pdf
KPMG International Third-Party Risk Management Outlook 2022	https://assets.kpmg/content/dam/kpmg/xx/pdf/2022/01/third-party-risk-management-outlook-2022.pdf