

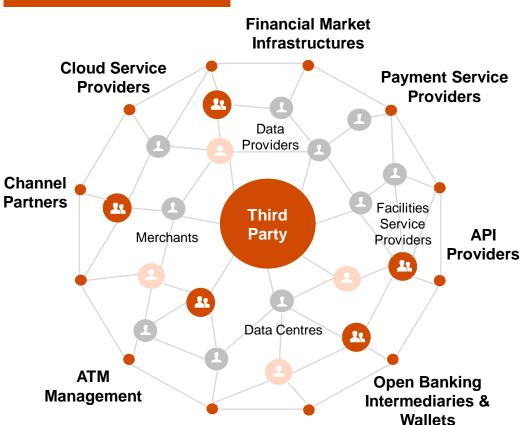
# Beyond Outsourcing – Elevate agility over broader Third Party Risk Management



In today's digitalisation landscape, banks and other financial institutions embrace more third party engagements to achieve straight through transactions and enhance customer experience. While these partnerships are vital for business success, they also introduce new risks that banks must address.

In the wake of recent events, a concerning surge in third-party incidents has emerged affecting numerous financial services across the world. The reverberating consequences of these breaches have underscored the urgent need for institutions to rethink Third Party Risk Management (TPRM) in their organisations.

### **Third-Party Landscape**





33% Increase in Cyber Attack

1 in every 10 organisations worldwide was hit by attempted Ransomware attacks in 2023.

Source: Check Point Research in 2023

**US\$1.2B** 

**Additional Regulatory Capital** Requirement

Additional capital and business suspension have been observed as regulatory penalties against Als after the banking services outages caused by third party disruption.

Source: BNN Bloomberg News



50% Increase

in Local Data Leakage Incidents

Increase of personal data breach incidents was driven by hacking and system misconfiguration, especially for outsourced data warehouses.

Source: Legislative Council Paper (Report on the work of PCPD in 2023)



In the past, financial institutions have been enforcing risk management over outsourcing arrangements. Until recent years, the regulatory landscape surrounding TPRM has evolved to cope with the emerging risks associated with increasing use of third parties that fall out of the scope of outsourcing.

### **United States**

Jun 2023, FDIC, FRB and OCC jointly issued final guidance "Interagency Guidance on Third-Party Relationships: Risk Management" on managing risks associated with third-party relationships, followed by a toolkit for enhancing third-party risk management and oversight in Dec 2023.

### **United Kingdom**

Mar 2021, PRA publishes the Supervisory Statement on Outsourcing and third party risk management (SS2/21), alongside with the Statement on Operational Resilience to set forth the regulatory expectations relating to outsourcing and third party risk management.

### **Singapore**

Aug 2022, MAS published the Information Paper on Operational Risk Management - Management of Third Party Arrangements and outlines the different expectations on operational risk, technology risk and business continuity management in relation to outsourcing and third-party risk management.

### **European Union**

Jan 2024, ESAs publish first batch of final draft regulatory technical standards under the Digital Operations Resilience Act (DORA) for ICT and third-party risk management and incident classification in relation to the financial entities' use of ICT third-party service providers.

### **Australia**

Jul 2023, APRA announced the new Prudential Standard CPS 230 Operational Risk Management will replace existing standards including the Prudential Standard CPS 231 Outsourcing (CPS 231) developed in 2017, to enhances third-party risk management by extending the requirements to cover all material service providers

**Hong Kong** 

### **Objectives of TPRM**



### **Minimise Compliance Risk**

- Ensure complying with applicable laws when engaging service providers
- Reduce chance of disruption on critical operations caused by third parties



### **Achieve Cost Optimisation**

- Centralize contracting process on a single platform
- Streamline and standardize third party engagement process to increase efficiency



### **Strengthen Cybersecurity**

- Identify, assess and mitigate cyber risks throughout the third parties lifecycle
- Expand cyber threat intelligence monitoring to cover key third-parties



### Third Party Risk Management Framework & Lifecycle

The nature and scope of third party risk management have been evolving over time, following is the example on the TPRM framework & lifecycle:

## **TRRM Framework Board & Senior Management Committee** Three Lines of Defense Risk-based **Business Units Risk Management Functions** Internal Audit TRRM Lifecycle



1. Risk Assessment

2. TP Due Diligence & Selection

3. Contracting

4. On-going Risk Monitoring

5. Termination









Conduct comprehensive risk assessment from bank-wide perspective on the proposed TP arrangement, covering:

- Importance of service/ function to be involved in TP arrangement
- Cost and benefit analysis
- Impact on the bank's risk profile



Perform due diligence assessment on potential third parties based on various factors, including third parties' service quality, business reputation and business continuity planning, etc.

Based on due diligence assessment result, select the third party to be engaged



Incorporate SLAs and clauses on compliance, confidentiality, data protection and ethics into contracts for assurance of supply stability and quality, as well as mitigation of threats to banks.

Adopt adequate processes and robust central repository to standardise contracts prior to signing



**Centralised control** function reviews and mitigates risks associated with third-party arrangement

Utilise tools to evaluate concentration risk and monitor the performance of third parties, such as:

- Concentration risk analyses
- KRIs
- Heatmap



**Smooth transition** procedures such as transferring data, assets, or responsibilities and completing any outstanding work to avoid legal, financial, or operational risks or damages

Execute exit plan such as contract review, notice of termination, third party replacement.

### Potential Enhancement for TPRM

### **Key Dimensions of potential TPRM enhancement**

 Implement E2E lifecycle tools and analytics to manage the full life cycle of third party arrangements, including a central repository and data management system

 Implement third-party KRIs to monitor the performance of the third party arrangements, including service level agreement breaches, vendor incidents, regulatory breaches, expired contracts, overdue reviews/control tasks

 Conduct concentration risk analysis at the individual service provider level and bank-wide level to assess if the Bank has any excessive reliance on the service provider

Systematic
Lifecycle of
TRRM

Third Party Risk
Management

Risk-based
approach

Concentration risk analysis

 Establish a proper governance structure and framework for adequate management oversight and attention on risks arising from third party arrangements, including engagement from the Board and senior management and a centralised governance committee

> Establish and maintain a centralised third party inventory to streamline third party management, including to effectively identify, assess, and mitigate risks associated with third-party relationships.

Determine the level of controls required based on the risk level inherent to the corresponding third parties through materiality assessment and risk ratings over the third party relationship,



How PwC can support you...

## **Ensure Regulatory Compliance through Independent Assessment**

Perform comprehensive review on third party risk management to assess effectiveness of the Bank's processes and controls related to managing third party relationships and ensure relevant regulatory compliance, assessment aspects including:

- · Scope coverage of third parties
- · Risk management effectiveness
- Operational resilience in relation to third party management, e.g. incident response and contingency plans

## Establish a Holistic Framework with Future Operating Model

Develop a comprehensive framework for managing third-party risks within the Bank, encompassing the following aspects:

- Set up of third party risk management framework and governance structure
- Design of target operating model and definition on roles and responsibilities
- Establishment of policies and procedures regarding on third party risk
- Lifecycle management on third party arrangements

## Deploy Robust Tools with Streamlined Implementation

Integrate analytical tools and digital strategies into third party risk management:

- Definition of risk metrics for ongoing monitoring, e.g. risk appetite, key risk indicators (KRI), etc.
- Establishment of inherent risk rating for risk segmentation of third parties
- · Concentration analysis of third party portfolio
- Connectivity and synchronisation between third party contract management and procurement system
- Integrated digital dashboard to configure and enhance TPRM process covering due diligence and monitoring of control tasks and performance metrics



### **Call for action!**

Start your journey to mitigate third-party risk within the institution and enhance operational resilience in managing third-party risk.

### Contact us

### **James Tam**

Banking and Capital Markets Leader, PwC Hong Kong +852 2289 2706 james.tam@hk.pwc.com

### **Gary Ng**

Partner, PwC Hong Kong +852 2289 2967 gary.kh.ng@hk.pwc.com

### Karen Wong

Partner, PwC Hong Kong +852 2289 2571 karen.tw.wong@hk.pwc.com

#### Ho Kee Fu

Partner, PwC Hong Kong +852 2289 2721 ho.kee.fu@hk.pwc.com

#### Ross Xiao

Partner, PwC Hong Kong +852 2289 8425 ross.xiao@hk.pwc.com

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

© 2024 PwC. All rights reserved. In this document, PwC refers to the Hong Kong member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see <a href="https://www.pwc.com/structure">www.pwc.com/structure</a> for further details.