HONG KONG MONETARY AUTHORITY

Research Memorandum 11/2025

26 September 2025

Assessing the Information Communications and Technology Third-party Dependencies of Financial Institutions in the Asia Pacific Region: An Analysis of Business Relationship Data

***Key points*:**

- *The growing digitalisation of the financial industry has made financial institutions (FIs) more dependent on information communications and technology third-party providers (TPPs), potentially exposing them to higher systemic operational risks, as service disruptions to major TPPs could affect the operations of a large number of FIs.*

- *To shed light on this issue, this study gauges the extent of dependency of FIs on TPPs in the Asia Pacific (APAC) region based on publicly available business relationship data obtained from a commercial database. To obtain a clearer picture of FIs' dependencies on TPPs, the analysis considers not only TPPs directly used by FIs ('direct TPPs') but also indirect dependencies arising from TPPs used by FIs' direct TPPs ('indirect TPPs').*

- *Our analysis shows that FIs in the APAC region are exposed to operational risks arising from both direct and indirect TPP dependencies. Notably, indirect TPP dependencies constitute a more important channel through which operational risks can be transmitted to FIs in the APAC region.*

- *Further analysis also finds signs of concentration risks associated with FIs' TPP dependencies. Specifically, the 50 most dominant TPPs, ranked by the total number of FIs that rely on them directly or indirectly, serve half of our sampled FIs. Despite the lack of granular information to account for the criticality of these TPPs' services, this result suggests that the potential systemic risks arising from disruptions to dominant TPPs could be widespread, warranting close monitoring.*

- *Moreover, most dominant TPPs are headquartered outside the APAC region, suggesting that disruptions to these TPPs could generate significant cross-border spillover effects on FIs in the region. This result highlights the importance of enhancing the monitoring of risks arising from FIs' cross-border dependencies on TPPs.*

- *However, we find that FIs in the region tend to select TPPs with relatively higher cybersecurity risk management quality, which can partly mitigate the risks. In addition, our analysis reveals a strong positive correlation between the quality of FIs' cybersecurity risk management and that of their TPPs. This reflects that FIs with better cybersecurity risk management have greater incentives and ability to select higher quality TPPs. This finding underscores the importance of enhancing FIs' cybersecurity risk management.*

- *Finally, it is important to note that data limitations prevent a full assessment of this issue, as some key attributes related to the extent of FIs' dependencies on TPPs, such as the criticality and substitutability of their services to FIs' operations, cannot be fully accounted for in our analysis. Therefore, caution should be exercised when interpreting the findings of our study.*

*Prepared by: Andrew Wong, Kelvin Ho, Icarus Chan**

Market Research Division, Research Department

Hong Kong Monetary Authority

The views and analysis expressed in this paper are those of the authors, and do not necessarily represent the views of the Hong Kong Monetary Authority.

* The authors would like to thank Eric Wong for his helpful comments and suggestions.

I. Introduction

The growing digitalisation in the financial services industry has led to an increased dependency of financial institutions (FIs) on information communications and technology (ICT) third-party service providers (hereafter referred to as ‘third-party providers’, TPPs). Although the adoption of services from these TPPs may enhance the quality of services offered to clients and promote operational efficiency, this trend may have implications for systemic operational risks, as service disruptions to major TPPs could affect the operations of a large number of FIs.

Systemic operational risk has received increasing attention from policymakers and business executives due to the rising number of cyber incidents at FIs’ service providers, which in turn can have direct repercussions on their business. In 2024 and 2025, many FIs around the world[1] faced cyber incidents associated with the use of TPPs in their business. In addition, around 54% of large firms’ business executives cited third-party risk management as a major challenge in a survey published by the World Economic Forum (WEF, 2025).

In response to the emergence of operational risk due to TPP dependencies, the Financial Stability Board (FSB) published a toolkit document in 2023 with the aim of helping ‘*strengthen financial institutions’ ability to manage third-party risks and financial authorities’ ability to monitor and strengthen the resilience of the financial system*’ (FSB 2023, page 3). Despite the importance of this issue, there are few quantitative assessments to examine the extent of TPPs (particularly in the Asia Pacific (APAC) region), reflecting the difficulties in collecting relevant data for a broader market assessment.[2]

In this context, this study aims to shed light on this issue in the financial services industry of the APAC region. Using publicly available business relationship data obtained from S&P Capital IQ, we aim to gauge the extent of FIs’ dependencies on ICT TPPs in the APAC region. Specifically, we focus on the following questions:

[1] For instance, a software attack on a US bank, a supply chain cyberattack on Swiss banks, a ransomware attack on a vendor of some APAC banks, and a ransomware attack on an external vendor engaged by an insurer in Singapore.

[2] A recent study that addresses this issue is that of the IMF (2024). This study measures the share of third-party IT suppliers concurrently used by global systemically important banks and major global insurers to explore potential sources of common shocks to the financial system.

1. **TPP Dependency**: measuring the extent of TPP dependency of FIs in the APAC region, by TPP type and geographic location;
2. **Concentration risk**: assessing the degree of concentration risk on TPP dependency in the financial industry of the APAC region;
3. **Quality of cybersecurity risk management of TPPs adopted by FIs**: analysing whether FIs take into account the quality of cybersecurity risk management of TPPs when selecting their TPPs.

By addressing these questions, our study may shed light on the degree of concentration risk and cross-regional geographic exposure to TPP dependencies within the financial industry of the APAC region. These findings should be highly relevant to policymakers when gauging potential systemic operational risks arising from FIs' TPP dependencies.

The remainder of this paper is organised as follows. Section II describes the data and methodology used in the study. Section III presents our findings regarding the extent of ICT TPP dependencies of FIs in the APAC region. Section IV presents our empirical findings regarding whether FIs take into account the quality of cybersecurity risk management of TPPs when selecting their TPPs. Finally, Section V concludes the study.

II. Data and methodology

In this section, we provide a brief overview of the data sources and relevant terminology used in the analysis.

2.1 Business relationship data from S&P Capital IQ

Our primary source of customer–supplier business relationship data is S&P Capital IQ. This dataset captures the business relationships of FIs reported over the past two years. To identify relevant TPPs deemed relevant to this study, we use generative artificial intelligence (GenAI) to analyse their business descriptions and industry classifications for more accurate identification.[3]

To better distinguish the types of ICT services provided by these TPPs, we first define six major classes of ICT TPPs (Table 1).[4] We then use GenAI to classify a TPP into one of these six pre-defined ICT cyber agent classes (hereafter, 'classes'). Details about each TPP class and how GenAI conducts the classification task are presented in Appendix A.1.

Table 1: TPP Classes

Cloud service provider	Telecommunications technology service provider
IT system and software service provider	IT hardware provider
Cybersecurity service provider	Digital financial services and financial products provider

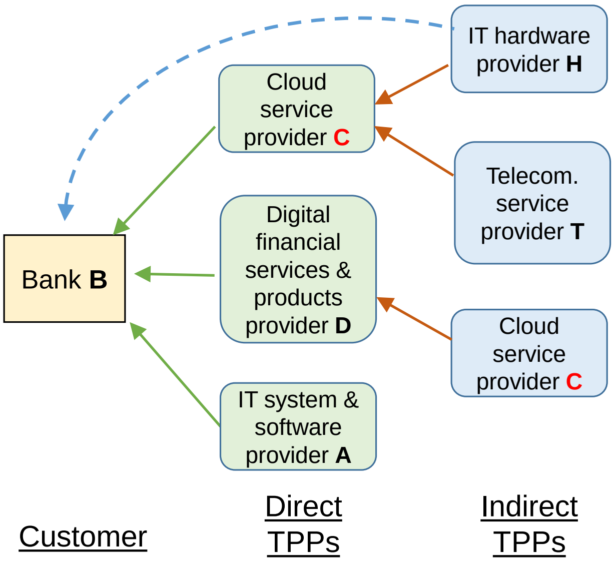
It is important to note that there are two types of TPP dependencies: direct dependencies and indirect dependencies. Chart 1 presents a hypothetical example: a direct dependency arises when Bank B uses the cloud storage service of TPP C. If TPP C uses third-party ICT hardware provider H, then Bank B has an indirect dependency on TPP H through the business relationship between cloud TPP C and hardware TPP H.[5] We assess both direct and indirect dependencies in our analysis.

[3] As we focus on assessing the extent of FIs' ICT TPP dependencies, we only retain a subset of business relationships categorised as 'supplier' and 'vendor' types, and remove all business relationships in which both customers and suppliers belong to the same parent holding companies.

[4] We follow Wilson et al. (2019), Brauchle et al. (2020), and EBA (2023) to compile the list of TPP classes to better differentiate their economic activities.

[5] Another important aspect of this example is that Bank B has both direct and indirect dependencies with cloud service provider C, highlighting the complexity of the different types of dependencies that can exist within the ICT supply chain in practice.

Chart 1: An illustrative example of a bank's direct and indirect TPP dependencies



To construct our analytical sample, we first collect a sample of FIs from the APAC region with business relationship data reported in our data source. The sample includes 1,145 FIs from four major types of financial companies. Among them, 33% are banks, 24% are capital market institutions, 27% are financial services companies, and 16% are insurance companies. For each FI, we first identify their direct TPPs and then focus on the direct TPPs for which we can identify indirect TPPs for the sampled FIs in the APAC region.[6] One caveat in our identification of indirect TPPs is that due to the lack of information on the specific services or functions provided by each TPP, we cannot assess the criticality of indirect TPPs in supporting the services provided by direct TPPs to FIs.

Our final sample includes 3,667 direct TPPs and 13,960 indirect TPPs for the sampled FIs in the APAC region. Our TPP sample includes 1,466 unique ICT firms. Among them, around 42%, 22%, and 22% are classified as ICT system and software providers, cloud service providers, and digital financial services and products providers, respectively. The remaining 15% consist of ICT hardware, telecommunications technology service, and cybersecurity service

[6] In principle, the chain of indirect dependency could be extended further. To keep our analysis tractable, the indirect dependency of FIs is only captured up to "fourth party" service providers.

providers. Selected financial statement variables, including geographic locations of FIs and ICT TPPs, are obtained from S&P Capital IQ.

2.2 Measure of the quality of cybersecurity risk management

We measure the quality of cybersecurity risk management of FIs and their TPPs by the overall Information Security/Cybersecurity & System Availability component score derived from the S&P Corporate Sustainability Assessment methodology[7] (denoted as cybersecurity score) as of calendar year 2022 and 2023. The score ranges from 0 to 100, with a higher score indicating better quality of cybersecurity risk management.

Our analysis has some data limitations. For instance, some key attributes, such as the materiality of TPP services to FI operations, the nature of services provided by TPPs, and the substitutability of a business relationship, cannot be fully accounted for in our analysis because this information is not available in our dataset. This prevents us from conducting a complete assessment. Thus, caution should be exercised when interpreting our findings.

III. Analysis of the extent of FIs' dependencies on TPPs

We assess the extent of FIs' dependencies on TPPs from different perspectives: the degree of direct and indirect dependencies, the extent of concentration risk, and the associated cross-border spillover risks to FIs due to these dependencies.

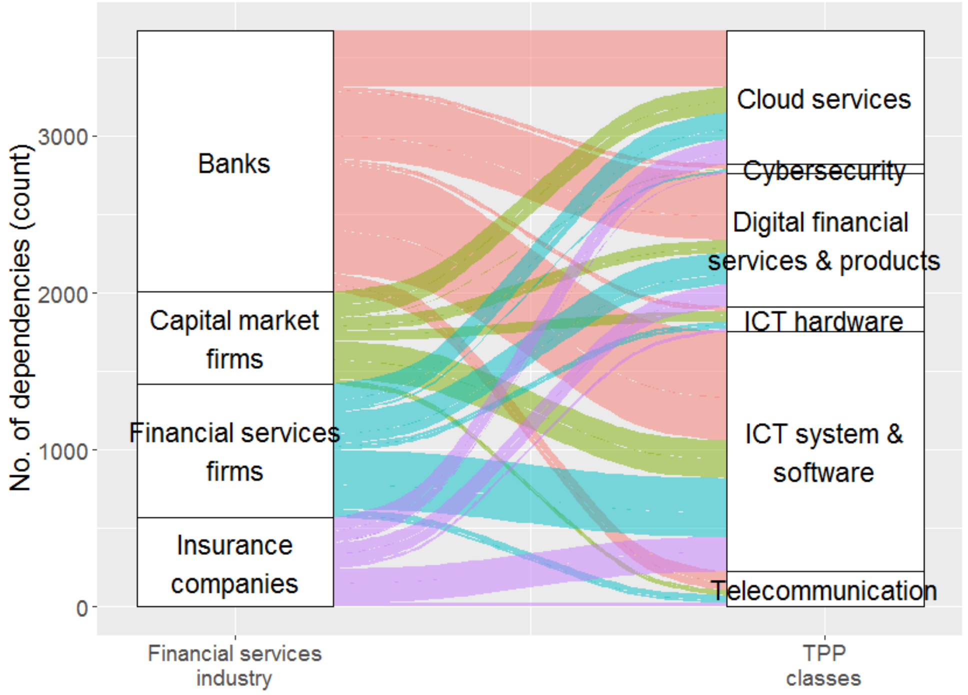
3.1 Assessing the extent of direct TPP dependencies of FIs in the APAC region

For direct TPP dependencies, Chart 2 presents the number of direct TPP dependencies by FI type. Banks have the largest number of direct TPP dependencies, accounting for 45% of all direct dependencies, followed by

[7] S&P Global assesses the sustainability dimensions of a large number of globally listed firms to produce CSA scores (ranging between 0 and 100) based on a firm's responses to questionnaires administered directly by the company each calendar year. The 'Information Security/Cybersecurity and System Availability' dimension of the CSA scores applies to all industries and includes questions about a firm's IT security governance, policy measures, and processes and infrastructure. For details, please read the S&P Global methodology documents.

financial services firms (23%), capital market firms, and insurance companies (16% each).

Chart 2: Number of direct TPP dependencies of FIs (by type of FI and TPP)



Note: The chart presents the number of dependencies between each FI industry group in the APAC region and their direct TPPs segmented by their TPP classes.

By TPP type, ICT system and software providers account for approximately 42% of all direct dependencies. This is followed by digital financial services and products providers and cloud service providers (23% each), ICT hardware service providers (4%), and telecommunications technology providers (6%). FIs' dependency on cybersecurity firms is relatively low, partly because cybersecurity firms and FIs tend not to disclose information about their business relationships.[8]

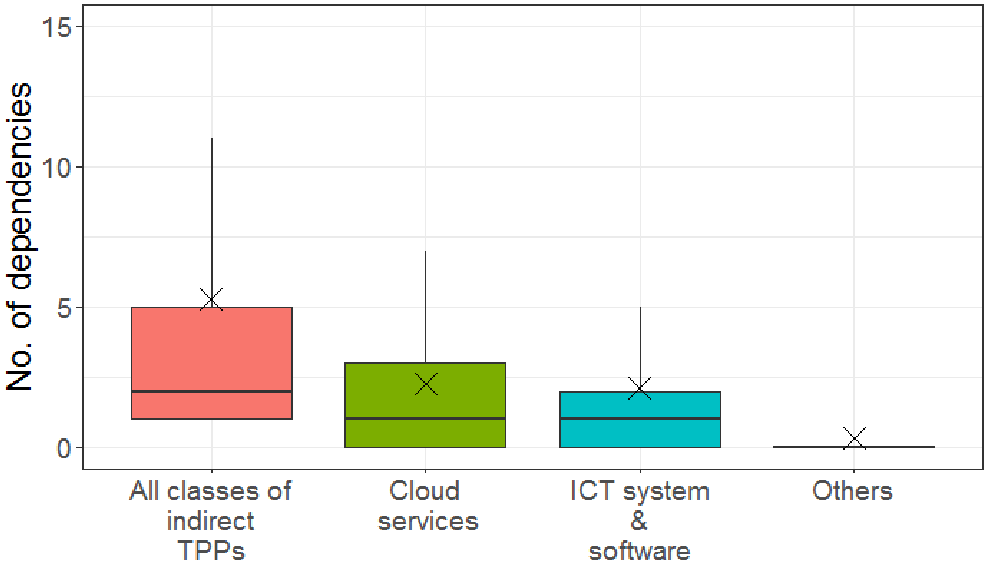
3.2 *Assessing the extent of indirect dependencies with ICT suppliers arising from the IT supply chain*

To assess the extent of indirect TPP dependencies, we focus on the TPPs used by the direct TPPs of our sampled FIs (i.e. the sample of ICT suppliers in

[8] Ernest and Young reveals that Fortune 100 companies rarely disclose their collaboration with peers, industry groups, or policymakers on cybersecurity risk management. (October 2024).

Chart 2).[9] Chart 3 shows that FIs' direct TPPs have on average dependencies with about 5 indirect TPPs (i.e. the orange boxplot). Similar to the pattern observed among FIs' direct TPP dependencies, cloud service providers and ICT system and software service providers are the two important types of indirect TPPs for our sampled direct TPPs.

Chart 3: Number of dependencies of direct TPPs on indirect TPPs



Note: The chart shows the distribution of dependencies of direct TPPs on indirect TPPs. The boxplot on the far left includes all indirect TPP classes, while the other boxplots present the distributions for selected TPP classes. In each boxplot, the black cross, the rectangular box, and the whisker line above the box represent the mean value and the interquartile ranges for each distribution.

Chart 4 presents the number of direct and indirect dependencies with TPPs by type of financial firm. The percentages in the blue and orange bars represent the share of direct and indirect TPP dependencies, respectively, of the four major FI groups in the APAC region.

[9] We omit TPPs identified as 'digital financial services and financial products providers' in our analysis of indirect TPP dependencies because the nature of their services provided to direct TPPs is unclear.

Chart 4: Number of direct and indirect dependencies with TPPs by FI type in the APAC region

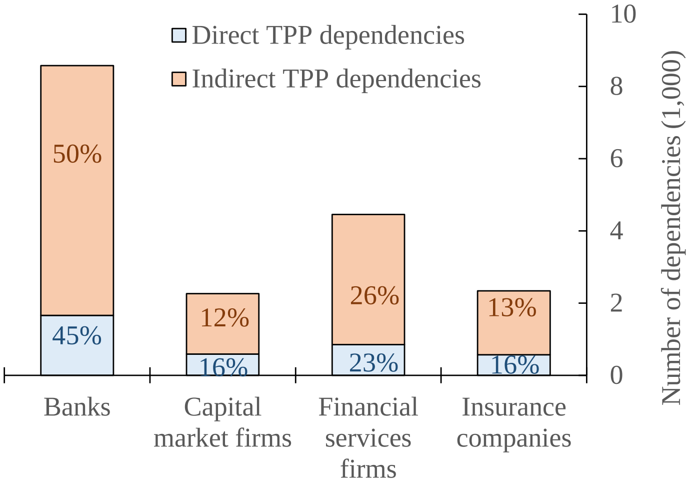


Chart 4 shows significant indirect dependencies on TPPs, particularly for banks. Specifically, the degree of FIs' indirect dependency on TPPs is three times higher than that of their direct dependency. This finding suggests that indirect TPP dependencies may be a major channel through which operational risks can be transmitted to FIs in the APAC region.[10]

3.3 *Assessing the extent of concentration risk*

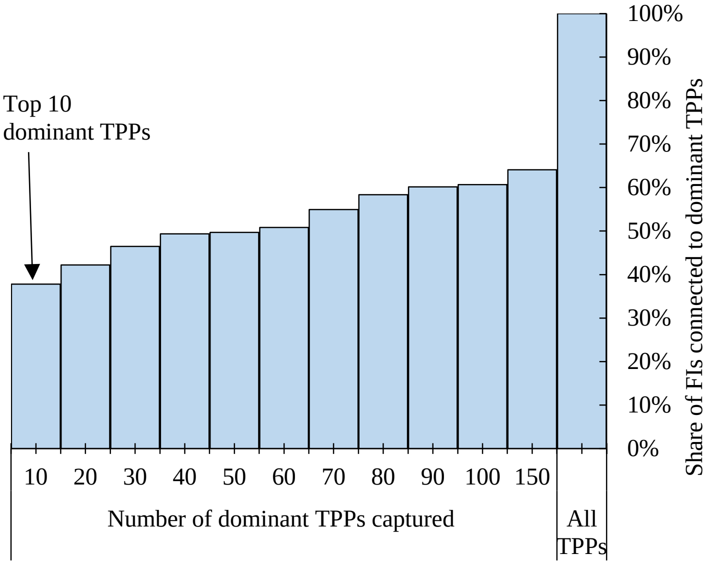
One concern regarding TPP dependencies is the potential for concentration risk, as heavy reliance on a few dominant TPPs can expose many FIs to significant operational risk if a dominant TPP experiences a service disruption.

To gauge this concentration risk, we calculate the cumulative share of FIs served by the most dominant TPPs, ranking them by the total number of FIs that rely on them directly or indirectly. Chart 5 reveals that concentration risk can be significant for FIs in the APAC region. For instance, the 10 most dominant TPPs serve 38% of our sampled FIs, while the top 50 TPPs serve half of our sampled FIs. Despite the lack of granular information to account for the criticality of services from these dominant TPPs, this result suggests that potential systemic

[10] Another notable observation is that direct and indirect dependencies exist concurrently for around 4% of the FIs and TPPs in our sample. In these dependency pairs, the impact of a TPP service disruption could then be transmitted to an FI through multiple channels, including directly disrupting the FI and indirectly disrupting the FI by affecting other direct TPPs. Therefore, in line with the FSB (2023), it is important for individual FIs to pay attention to potential spillover risks related to their direct dependencies and the supply chain of relevant third-party services.

risks arising from disruptions to dominant TPPs could be widespread, warranting close monitoring.

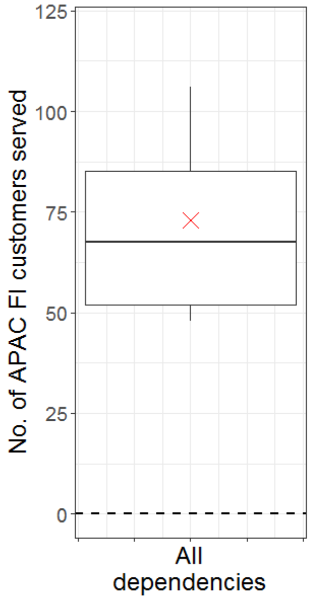
Chart 5: Cumulative share of FIs served by the most dominant TPPs



Although the likelihood of a simultaneous service disruption across multiple dominant TPPs is low, the potential operational risk to FIs resulting from a service disruption in any dominant TPP could still be significant if each TPP is adopted by a large number of FIs.[11] Chart 6 shows that on average, each dominant TPP among the top 50 TPPs serves (either directly or indirectly) 73 FIs in the APAC region, representing approximately 6.4% of our sampled FIs. This result suggests that even a disruption at a single dominant TPP could pose operational risks to a large number of FIs in the region.

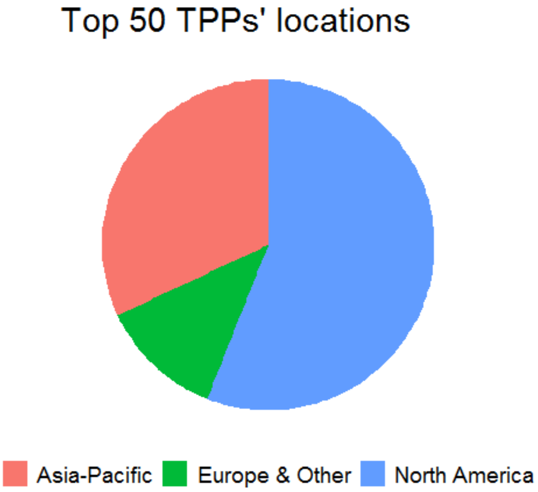
[11] As a real-life example, dozens of FIs worldwide were affected by the outage inflicted by CrowdStrike Inc. in July 2024.

Chart 6: Boxplot diagram of the number of FIs in the APAC region served by the top 50 ICT TPPs



Note: The chart shows the distribution of the number of FI customers in the APAC region for the top 50 TPPs identified in our sample, based on both direct and indirect dependencies. The rectangular box and the whisker lines extending from the box represent the interquartile ranges and the data points within 1.5 times the interquartile range above/below the 75th/25th percentiles, respectively. The red cross represents the average value of the distribution.

Chart 7: Geographic distribution of the top 50 dominant TPPs



Note: The geographic regions of the dominant TPPs are based on their headquarters jurisdictions, which are sourced from S&P Capital IQ.

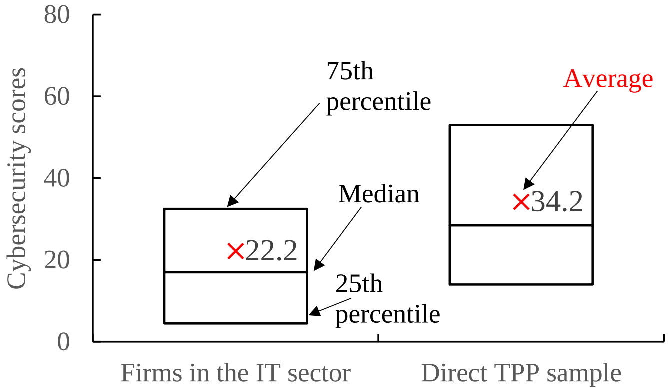
Moreover, Chart 7 shows that around two thirds of the top 50 dominant TPPs are non-APAC firms, suggesting that disruptions to these TPPs could have significant cross-border spillover effects on FIs in the APAC region. This finding suggests that it is important to enhance the monitoring of systemic operational risk arising from FIs' cross-border dependencies on TPPs (see relevant FSB recommendations (FSB, 2023)).

IV. To what extent is the quality of TPPs taken into account by FIs when selection their TPPs?

Although our previous analyses show that FIs are subject to operational risks arising from both direct and indirect TPP dependencies, the level of such risks depends critically on the quality of cybersecurity risk management of their TPPs.[12] As highlighted by the FSB (2023), the implementation of cybersecurity risk management measures by FIs or TPPs, including risk monitoring and the development of mitigation actions and plans, can help enhance operational resilience to cyber incidents and reduce the likelihood of service disruptions.

Comparing the cybersecurity score used in our study for the group of TPPs adopted by FIs in the APAC region with that of the entire information technology (IT) sector, anecdotal evidence suggests that FIs in the APAC region generally select TPPs with a relatively high quality of cybersecurity risk management. As shown in Chart 8, the average and median cybersecurity scores of our sampled TPPs are approximately 12 points higher than those of all firms in the IT sector.

Chart 8: Boxplot diagram of cybersecurity score distributions of firms in the IT sector versus the sample of direct TPPs



Note: The boxplots are calculated using data from 1,709 firms in the IT sector and 645 firms in the direct TPP sample. For each firm, cybersecurity score is the average values of the cybersecurity scores for the calendar years 2022 and 2023. The interquartile ranges in each distribution are represented by the rectangular boxes. Additionally, the average values in each distribution is indicated by the red crosses, with corresponding figures reported next to them.

[12] In addition to the quality of cybersecurity risk management, it is important to consider the financial resilience of FIs' TPPs, as any deteriorations in the financial soundness of these providers could compromise the continuity of their service delivery. In general, we find that the majority of TPPs used by FIs in the APAC region are financially sound, suggesting that financial vulnerability should not pose a major challenge to their operational continuity at this time.

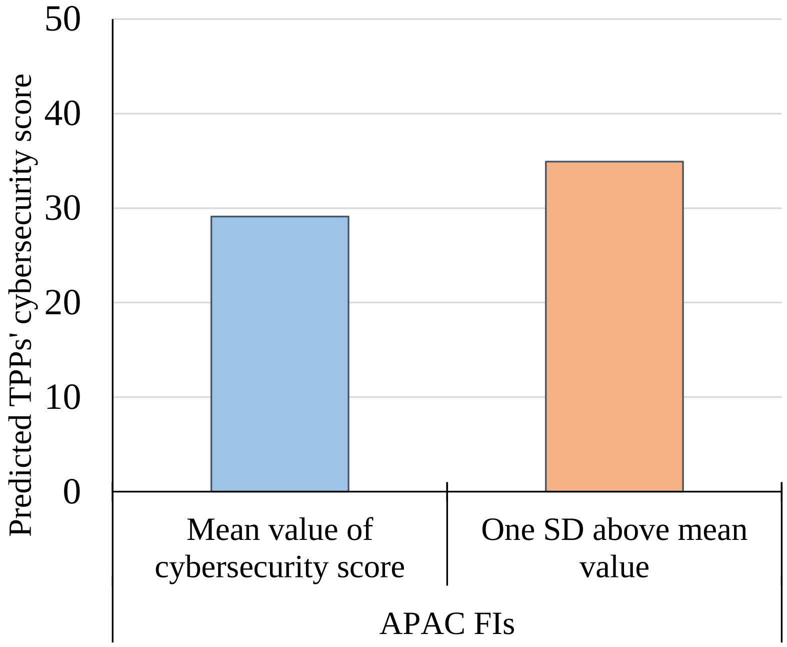
We also use a simple regression model to estimate the statistical relationship between FIs’ cybersecurity score (as the independent variable) and the average value of the cybersecurity scores of their direct TPPs (as the dependent variable).[13] If FIs with better cybersecurity risk management do place greater importance on the quality of their TPPs’ cybersecurity risk management in their selection process, we expect to find a positive correlation between the two variables mentioned above. Details on the empirical specifications and estimation results are provided in Appendix A.2. As cybersecurity scores are only available for a subset of FIs in the APAC region (about 25% of the sampled FIs covered in Section III), we also conduct a robustness check based on a global sample of FIs.

Based on a sample of 286 FIs in the APAC region, we find a positive and statistically significant relationship between our two variables of interest. This result is consistent with our conjecture that FIs with better cybersecurity risk management have greater incentives and ability to select higher quality TPPs. The impact is also economically significant. Specifically, a one standard deviation (SD) above the mean of FIs’ cybersecurity scores is associated with an average value of their TPPs’ cybersecurity scores that is 5.8 points higher, representing a 15% increase from the average score of 39 in our sample (Chart 8). The estimated impact is quantitatively similar based on a global sample of FIs, suggesting that our findings are robust and not driven by a small number of samples (see Appendix A.2).

As FIs with better cybersecurity risk management tend to select higher quality TPPs, this finding underscores the importance of enhancing FIs’ cybersecurity risk management, which can help promote greater operational resilience in the financial system.

[13] The average cybersecurity scores are based on the sample of TPPs with available cybersecurity scores.

Chart 9: Estimated effects of higher cybersecurity scores of FIs on the average cybersecurity scores of their TPPs



Note: The bar charts represent the estimated impacts of a one standard deviation (SD) increase in FIs' cybersecurity scores on their TPPs' cybersecurity scores based on our regression specification. For further details on this specification, please see Appendix A2.

V. Conclusion

The trend towards digitalisation in the financial industry has led to a significant dependency of FIs on ICT TPPs, potentially exposing them to higher systemic operational risks. Using customer–supplier business relationship data from S&P Capital IQ to gauge the extent of FIs' dependencies on TPPs, our findings show that FIs in the APAC region are exposed to operational risks arising from their direct and indirect TPP dependencies. Specifically, the degree of indirect dependency on TPPs is significantly higher than that of their direct dependency, suggesting that indirect TPP dependencies could constitute a significant channel through which operational risks can be transmitted to FIs in the APAC region.

Further analysis shows signs of concentration risks associated with FIs' TPP dependencies, with the top 50 dominant TPPs serving half of our sampled FIs. This result suggests that potential systemic risks arising from disruptions to dominant TPPs may be widespread and warrant close monitoring. Moreover, most of these dominant TPPs are headquartered outside the APAC region, suggesting that the potential cross-border impacts stemming from disruptions to these TPPs on the operational risks of FIs in the region could be significant, underscoring the importance of enhancing oversight of these cross-border TPP dependencies (see relevant discussions in FSB (2023)).

Nevertheless, the potential operational risks arising from TPP dependencies may be partially mitigated by the fact that FIs in the region tend to select TPPs of higher quality in terms of cybersecurity risk management. In addition, our analysis reveals a strong correlation between the quality of FIs' cybersecurity risk management and that of their TPPs, suggesting that FIs with better cybersecurity risk management have greater incentives and ability to select higher quality TPPs, thus reducing potential operational risks from their dependencies on TPPs. This underscores the importance of enhancing FIs' cybersecurity risk management. To this end, the HKMA has provided industry-specific guidance to assist Hong Kong banks in putting in place effective cybersecurity measures covering their own operations as well as their links with TPPs.[14]

Finally, it should be noted that data limitations prevent a full assessment of this issue, as some key attributes related to the extent of FIs' dependencies on TPPs, such as the criticality and substitutability of their services to FIs' operations, cannot be fully accounted for in our analysis. Therefore, caution should be exercised when interpreting the findings of our study.

[14] See the modules in the HKMA Supervisory Policy Manual, including "SPM TM-C-1 Supervisory Approach on Cyber Risk Management", "SPM OR-1 Operational Risk Management", "TM-G-1 General Principles for Technology Risk Management", and "OR-2 Operational Resilience".

Appendices

A1. GenAI classification of TPP classes

We use the Google Gemini 2.0 model, a proprietary large language model, to classify whether a supplier/vendor of an FI in a business relationship is a relevant TPP for this study. One advantage of this approach, compared with simply using the Global Industry Classification Standard for classification, is a broader coverage of different TPP classes, as firms in some classes are not classified into the typical information technology and telecommunications sectors.

Specifically, we provide detailed paragraphs on the six TPP classes in this study along with each company's business descriptions as supplementary information in the prompt for Gemini for processing. In addition, three examples are provided to Gemini 2.5 to apply the few-shot prompting technique to guide language model responses. If there is insufficient information about the company itself for classification based on the business descriptions determined by Gemini, we also examine the parent holding company's information and check its industry classification. The specific prompt is shown in Chart A1.

Chart A1: Prompt sent to the Google Gemini 2.5 model

You are a helpful assistant. Ensure your answers are complete, unless the user requests a more concise approach. When presented with inquiries seeking information, provide answers that reflect a deep understanding of the field, guaranteeing their correctness. For prompts involving reasoning, provide a clear explanation of each step in the reasoning process before presenting the final answer.

Your TASK is to classify a company into CLASSES of cyber network counterparties based on a given firm-specific business description.

There are six major CLASSES of cyber network counterparties, namely i.) ICT hardware provider; ii.) cybersecurity service provider; iii.) cloud service provider; iv). ICT system and software provider; v.) telecommunication technology service provider; vi.) digital financial service and digital financial products provider.

Supplementary information about each CLASS of cyber network counterparties is given for references.

An ICT hardware supplier is a company or entity that manufactures, distributes or supplies physical components and devices used in information and communication technology systems. This includes a wide range of products such as computers, servers, networking equipment, storage devices, and other electronic hardware that form the backbone of ICT infrastructure.

A cloud service provider is a company that offers some component of cloud computing that provides on-demand availability of computer system resources. This includes a range of service such as data storage and computing power, without direct active management by the user.

An ICT system and software service provider is a company or entity that offers services related to the development, implementation, management, and maintenance of information and communication technology systems and software. This includes designing and deploying software applications, providing cloud services, managing IT infrastructure, and delivering technical support and consultancy.

A cybersecurity service provider is a company or entity that offers services designed to protect information systems, networks, and data from cyber threats and unauthorized access. These services include risk assessment, threat detection and response, vulnerability management, security monitoring, incident response, and consultancy on security best practices.

A telecommunication service provider is a company or entity that offers services for transmitting voice, data, text, sound, and video across distances. The company will provide services such as telephony and data communications access and internet access service. These services are delivered through various technologies such as wired and wireless networks, satellite systems, and internet-based platforms. Electricity generation, supply and distribution is not included.

A digital financial service and digital financial products provider is a company or entity that offers financial services and products through digital platforms and technologies, which may include the applications of blockchain technologies in financial services. These providers leverage online and mobile channels to deliver a range of financial services, including banking, payments, lending, insurance, and investment management.

When answering, you should follow these rules.

Rule 1: If the company's business description is irrelevant to any of the six classes relevant to the aspect under the information communication technologies segment, you should return OTHERS.

Rule 2: One company may belong to multiple classes of these six classes, in this case, return all relevant classes.

Rule 3: In the case of multiple classes, you should rank the class of cyber network counterparties for the company by placing the most relevant classes in the first.

Rule 4: If you are uncertain of the class for the company based on the given business description, you will return UNKNOWN.

Rule 5: You should return the CLASSES after ### again at the end of your reply.

[INSERT Example 1]
[INSERT Example 2]
[INSERT Example 3]

You will be provided with a business description for a company below, which describes the company’s major business activities.

Business description: [INSERT Business description paragraph]

Classify this company.

A2. Empirical specification for the analysis of operational resilience factors in business relationships

We use the following cross-sectional regression specification (1) to estimate the impacts shown in Chart 9 in Section IV:

$$Average\ suppliers'\ Cybersecurity\ score\ _{i,22-23\ avg} = \boldsymbol{\beta_1 FIs'\ Cybersecurity\ score_{i,\ 22-23\ avg}} + No.of\ TPP\ linkages_i + ROA\ _i + Size\ _i + FE_{industry} + FE_{region} + \varepsilon_i \qquad (1)$$

The dependent variable $Average\ TPPs'\ Cybersecurity\ score\ _{i,22-23\ avg}$ is the average value of TPPs' cybersecurity scores for FI i. Our main explanatory variable is $FIs'\ Cybersecurity\ score_{i,\ 22-23\ avg}$, which is the S&P CSA score of FI i in the IT/Cyber/System Availability component between 2022 and 2023. β_1 is the parameter of interest that captures the impact of different levels of FIs' cybersecurity scores. In the regression, we control for the number of TPPs used by FI i, the size (logarithm of total assets in US dollar) and profitability of FI i, as well as region and industry fixed effects to control for any heterogeneity induced by differences in their financial metrics and unobserved industry characteristics. We estimate the same regression for a sample of global FIs and a smaller sample of APAC FIs only.

The summary statistics and estimation results are reported in Table A2.1 and Table A2.2, respectively.

Table A2.1: Summary statistics of variables

Variable	N	Mean	SD	P25	P50	P75
Average cybersecurity scores of TPPs linked to FI *i*	628	33.64	22.88	16.5	31.33	48.70
FI *i*'s cybersecurity score	628	40.23	26.94	18	37.5	60.5
No. of TPP relationships for FI *i*	628	4.7	6.37	1	2	5
ROA	628	2.147	3.07	0.576	1.201	2.747
Size	628	31.36	2.11	29.99	31.44	32.77

Table A2.2: Results of Regression (1) based on different samples

	(1)	(2)	(3)
Dependent variable	Average cybersecurity score of TPPs		
Independent variable			
FIs' cybersecurity score ($\boldsymbol{\beta_1}$)	0.1616***	0.1786***	0.1969*
	(0.0333)	(0.0359)	(0.0508)
No. of TPPs		0.1111	0.1539
		(0.0784)	(0.1480)
ROA		-0.1021	0.6584
		(0.4904)	(0.2823)
Size		-1.563**	-1.394
		(0.4270)	(0.5603)
Sample	Global F.I.	Global F.I.	APAC F.I.
No. of observations	628	628	286
Standard error type	I.I.D.	Region-industry	Industry
Region FE	No	Yes	No
Industry FE	No	Yes	Yes
R^2	0.0362	0.0793	0.0984

***, **, and * indicate statistical significance at the 0.001, 0.01, and 0.05 levels, respectively. The results in column (1) remain qualitatively similar if we replace the S&P CSA score with the S&P ESG score.

References

Baruchle J.-P., Gobel M., Seiler J., von Busekit C., 2020. "Cyber mapping the financial system", *Cyber Policy Initiative Working Paper Series*, No. 6, April 2020.

Ernest and Young (EY), 2024. "Cyber disclosures: what companies shared about cyber risks in 2024", *EY Center for Board Matters*, Report, October 2024.

European Banking Authority (EBA), 2023. *ESAs Report on the Landscape of ICT Third-party Providers in the EU*, Publication, jointly with European Insurance and Occupational Pensions Authority & European Securities and Markets Authority, 19 September 2023.

Financial Stability Board (FSB), 2023. *Enhancing Third-party Risk Management and Oversight*, Publication, 4 December 2023.

International Monetary Fund (IMF), 2024. "Chapter 3: Cyber risk: A growing concern for macro-financial stability", *Global Financial Stability Review*, April 2024.

Standard & Poor (S&P) Global, 2025. *CSA Methodology Handbook*, Methodology documents, S&P Global, March 2025.

Wilson C., Gaidosch T., Adelmann F., and Morozova A., 2019. "Cybersecurity risk supervision", *IMF Departmental Paper Series*, No. 19/15, April 2019.

World Economic Forum (WEF), 2025. *Global Cybersecurity Outlook 2025*, Report, 13 January 2025.