SAI360
RISK FROM EVERY ANGLE

# Your Guide to Third-Party Risk Management in Asia

## Table of Contents

# Introduction

Asia-Pacific financial institutions are rapidly reshaping how they source and deliver services, with a significant increase in the adoption of third-party technology. Between April 2023 and April 2024, banks in the region recorded the fastest growth in external tech use, outpacing North America, EMEA, and South America. This trend reflects a confluence of digital drivers: cloud migration, open banking mandates, and deepening integration of APIs and platform services.[1]

**Figure 1: Growth in third-party technology use (April 2023–April 2024)**

*(Scale: 0 = Minimal | 4 = Substantial)*

| Region | April 2023 | April 2024 | Change |
|---|---|---|---|
| Asia-Pacific | 2.53 | 3.14 | +0.60 |
| EMEA | 2.47 | 2.80 | +0.33 |
| North America | 2.74 | 3.22 | +0.48 |
| South America | 3.14 | 3.71 | +0.57 |

*Source: Guidewire. Banks and bank holding companies with revenue over $5 billion.*

Outsourcing delivers clear advantages—greater agility, scalability, and innovation. But it also intensifies operational and cyber risk exposure. Institutions are increasingly vulnerable to disruptions, security incidents, and compliance breakdowns rooted in third-party failures.

Regulators across Asia have acknowledged this evolving risk. Although their approach often leans toward principles-based guidance rather than prescriptive rulemaking, supervisory expectations are maturing and aligning with many global standards. The core regulatory themes will feel familiar to firms well-versed in European frameworks.

This paper explores these themes. It offers a practical blueprint for how Asian institutions can strengthen their third-party risk management (TPRM) to meet evolving regulatory expectations and build resilience in an increasingly interconnected financial ecosystem.

1. https://www.spglobal.com/ratings/en/research/articles/240704-cyber-risk-insights-fortifying-digital-defense-key-for-asia-pacific-banks-13167042#:~:text=The%20advent%20of%20open%20banking,business%20opportunities%20with%20fintech%20companies

# TPRM Regulation in Asia

Asian regulators are at different stages in formalizing TPRM rules, but financial hubs are leading the charge. Singapore and Hong Kong have emerged as regulatory benchmarks, offering relatively mature and detailed guidelines that extend beyond outsourcing to encompass broader themes of technology risk and operational resilience.

## Singapore: Detailed Expectations, Active Supervision

Singapore's Monetary Authority (MAS) has taken one of the most hands-on approaches in the region.

- Dec 2023: Notice 658 Management of Outsourced Relevant Services for Banks[2]
- Dec 2023: Notice 1121 Management of Outsourced Relevant Services for Merchant Banks[3]
- NEW Jan 2025: Guidelines on Outsourcing (Financial Institutions other than Banks)[4]

The guidelines reflect a clear shift toward supervisory accountability, emphasizing Board and senior management oversight, comprehensive due diligence, and an up-to-date outsourcing register.[5]

What sets MAS apart is its proactive supervisory posture. Thematic inspections are common, and MAS frequently publishes insights on good practices and observed deficiencies. TPRM is also embedded in broader operational risk management expectations,[6] reinforcing its strategic importance.

## Hong Kong: Principle-Driven but Pragmatic

The Hong Kong Monetary Authority (HKMA) takes a more principles-based approach. Its Supervisory Policy Manual SA-2 outlines expectations for maintaining operational control and protecting customers, even when functions are outsourced.[7]

Although non-statutory, the HKMA's guidance asks institutions to demonstrate outsourcing does not compromise governance, compliance, or resilience. It's a pragmatic model that trusts institutions to tailor controls within clear regulatory boundaries.

## Emerging Frameworks in the Region

- **Malaysia** has introduced foundational outsourcing rules via Bank Negara Malaysia, which are grounded in principles but lack the granular detail seen in Singapore or Hong Kong.[8]
- **Japan** outlined the Fundamental Elements for Third-Party Cyber Risk Management in the Financial Sector in October 2022.[9] The Financial Services Agency (FSA) expects financial institutions to maintain sound governance and risk management practices when engaging third parties, particularly in areas involving critical operations or customer data. While detailed, prescriptive rules are limited, supervisory reviews and expectations around operational resilience and data protection continue to evolve, signaling a gradual shift toward more structured third-party risk oversight.

2. https://www.mas.gov.sg/regulation/notices/notice-658
3. https://www.mas.gov.sg/regulation/notices/notice-1121
4. https://www.mas.gov.sg/-/media/mas-media-library/regulation/guidelines/bd/guidelines-on-outsourcing/guidelines-on-outsourcing---financial-institutions-other-than-banks.pdf
5. https://www.mas.gov.sg/-/media/mas-media-library/regulation/guidelines/bd/guidelines-on-outsourcing/guidelines-on-outsourcing-banks.pdf
6. https://www.mas.gov.sg/-/media/mas-media-library/publications/monographs-or-information-paper/imd/2022/operational-risk-management---management-of-third-party-arrangements.pdf
7. https://brdr.hkma.gov.hk/eng/doc-ldg/docId/getPdf/20011228-3-EN/SA-2.pdf
8. https://www.bnm.gov.my/-/policy-doc-outsourcing28122018#:~:text=The%20Bank%20today%20issued%20the,Business%20continuity%20planning.
9. https://www.fsa.go.jp/inter/etc/20221021/thirdparty_fe.pdf

## TPRM Expectations

Each referenced nation prescribes a similar TPRM framework, requiring top-down accountability and rigorous lifecycle oversight from due diligence to exit. Six foundational components of TPRM emerge from these regional regulators.

### 1. Responsibilities of the Board and Senior Management

Outsourcing may delegate operational tasks to organizational extremities, but never accountability. The institution must manage risk as if the function were performed internally.

> "Outsourcing can only allow [institutions] to transfer their day-to-day managerial responsibility, but not accountability, for an activity or a function to a service provider."[10]

The HKMA's principles-based approach allows for flexibility in implementation but places the burden of oversight firmly on the Board and senior management.

In contrast, Singapore's Monetary Authority takes a more prescriptive stance. Its guidelines delineate a clear division of labor between the Board and senior management, covering everything from policy approval and risk evaluation to business continuity and audit oversight.

### 2. Risk Management Framework

Leaders need confidence that outsourcing delivers strategic value without compromising control, resilience, or compliance. Before entering any material outsourcing arrangement, especially for IT services, firms must conduct a comprehensive risk assessment.

At its core, this risk assessment is a reality check: Does the benefit of outsourcing truly outweigh the risk? If not, how can we improve the risk-reward equation?

### 3. Regulatory Expectations for Risk Assessments:

- **Strategic alignment –** Ensure the outsourcing supports business goals, not just cost or efficiency gains
- **Due diligence –** Understand the arrangement's scope, complexity, and risks before making a commitment
- **Service provider assessment –** Confirm the vendor can meet regulatory, performance, and control expectations
- **Risk profile analysis –** Gauge how outsourcing changes your overall risk exposure, and whether you have the internal capability to manage that shift
- **Concentration risk –** Avoid over-reliance on a single provider, jurisdiction, or technology stack

10. https://brdr.hkma.gov.hk/eng/doc-ldg/docId/getPdf/20011228-3-EN/SA-2.pdf

## 4. Due Diligence

Thorough due diligence is essential when considering, renegotiating, or renewing an outsourcing arrangement. The breadth and depth of assessment matter, and the process should involve both an inside-out and outside-in assessment of the vendor's risk profile. This ensures informed decision-making, prioritization of oversight, and ongoing monitoring. Done well, due diligence helps firms understand which vendor relationships carry the most material risk.

## 5. Inside-out: Can they deliver safely and reliably?

Assess the vendor's internal capabilities with the same scrutiny you would apply to your organization's:

- **Governance and financial health**
- **Cybersecurity and operational resilience**
- **Compliance readiness and regulatory track record**
- **Internal controls, audit mechanisms, and staff integrity**

## 6. Outside-in: What's happening in their environment?

Look beyond the vendor to the broader ecosystem:

- **Geopolitical, legal, and regulatory risks** in their home jurisdiction
- **Reputational exposure** based on history or public perception
- **Third-party dependencies** (i.e., their own subcontractors and supply chain)

### Track What Matters

Maintain a comprehensive inventory of all outsourced services and underlying dependencies. This supports visibility, incident response, and regulatory reporting, ensuring no critical exposure falls through the cracks. Inventories must be submitted to regulators at specific intervals, such as semiannually in Singapore and Hong Kong.

## Outsourcing Agreements

Outsourcing agreements should clearly define both parties' roles, responsibilities, and expectations and be reviewed by qualified legal counsel to ensure enforceability. Each agreement should address the risks identified during due diligence and allow for timely renegotiation or renewal, enabling the bank to maintain sufficient control and intervene as needed to meet legal and regulatory obligations.

**Core contractual expectations:**

**1. Scope and standards**

- Clearly define the services, performance metrics, and internal control standards, as if the activity were performed in-house
- Embed service levels and key risk indicators (KRIs) that are measurable and enforceable

**2. Data protection and confidentiality**

- Include obligations to protect customer and internal data, as well as requirements for data destruction upon exit
- Pay special attention to cross-border data flows and local privacy laws

**3. Business continuity and recovery**

- Define the provider's responsibilities during service disruptions, including disaster recovery timeframes and fallback procedures

**4. Oversight and audit rights**

- Reserve the right to monitor, inspect, and audit the service provider and its subcontractors if applicable
- Include provisions for participation in regulatory audits or inspections

**5. Incident and breach reporting**

- Prompt notification of any material incidents, such as security breaches, service failures, or regulatory issues, is required to allow for timely mitigation and a regulatory response

**6. Exit and dispute resolution**

- Set out early termination rights, default events, transition assistance, and indemnities to enable orderly exit or transfer of services if needed
- Clearly define applicable law and jurisdiction, especially in cross-border contexts

**7. Subcontracting controls**

- Contracts should require prior approval for material subcontracting and hold the primary provider fully accountable for the compliance and performance of its subcontractors

## Ongoing Monitoring

Effective oversight begins with maintaining an accurate and up-to-date register of all outsourcing activities. Oversight shouldn't be siloed—many firms now establish cross-functional outsourcing management groups that bring together risk, legal, IT, compliance, and procurement to collectively assess provider performance and emerging issues.

Monitoring should occur both before and after implementation. Pre-implementation reviews assess whether controls are effectively embedded from the outset, while post-implementation reviews evaluate how well those controls perform in real-world conditions. Institutions should continuously track service level agreements (SLAs) and KRIs, particularly those related to data segregation and operational resilience—areas Asian regulators are increasingly focusing on.

Regular audits and independent assessments remain critical tools for validating controls and uncovering gaps. Just as importantly, institutions must have clear escalation and remediation protocols in place. When issues arise—be it a data breach, performance shortfall, or compliance lapse—timely escalation to senior management and, where appropriate, to the Board is essential. In high-risk or highly integrated arrangements, deeper engagement is expected. This includes frequent dialogue with providers, scenario testing, and joint exercises to test recovery and continuity plans.

## Business Continuity Planning

Outsourced IT services are often business-critical, making continuity and exit planning essential. Regulators emphasize the importance of well-tested contingency arrangements that enable seamless transition or rapid service restoration.

This includes Business Continuity Plans (BCPs) and Disaster Recovery Plans (DRPs) for both the service provider and the institution. In the event of service disruption or termination, institutions must retrieve or securely erase their data, shift operations to an alternative provider, or bring the service in-house.

# Future-Proof Your TPRM Framework

The complexity and interconnectedness of modern supply chains have outpaced traditional risk management approaches. While regional regulatory guidance on TPRM may be non-binding, it cannot be treated as optional. Escalating operational failures, data breaches, and service disruptions underscore the urgency to move beyond compliance and build future-ready, resilient TPRM frameworks.

## A Confluence of Risk

### Expanding Vendor Ecosystems Create Blind Spots

More than half of Singaporean organizations have not prioritized supply chain cybersecurity risk management, despite over 70% reporting breaches impacting their operations in 2024.[11] This highlights a persistent and worsening visibility problem, with many firms either unaware of or unable to monitor the risks lurking within their extended vendor networks.

Across Asia, supply chains are vast and deeply interconnected, often spanning multiple tiers of vendors and sub-vendors. This complexity makes achieving accurate end-to-end visibility a significant challenge. Traditional vendor mapping efforts are frequently undermined by incomplete, outdated, or inconsistent data. As a result, organizations remain exposed to risks from obscure downstream providers, many of whom fall far beyond their immediate oversight. Yet accountability still rests with the firm, regardless of how far removed the source of failure may be.

### Emerging Technologies Introducing New Risk Vectors

Generative AI and machine learning models are increasingly integrated into banking, fintech, and IT solutions, often provided by third-party vendors. The breakneck adoption of AI and other emerging technologies is introducing third-party risk vectors that traditional compliance checklists are ill-equipped to address. Asian regulators have expressed concern about financial institutions' heavy dependence on AI and third-party IT, cautioning that it could amplify cyber vulnerabilities across interconnected systems.[12]

TPRM practices must evolve to evaluate AI-related risks. This means going beyond standard vendor due diligence to ask new questions:

- How is the vendor using AI on our data?
- What controls and transparency exist around those AI systems?
- Are there safeguards against bias, error, or cyberattack in the vendor's AI pipeline?

Traditional TPRM guidelines in Asia offer little precedent here, so organizations themselves must raise the bar.

### Escalating Cyber Threats via Third Parties

At the same time, cyber threats continue to surge, and attackers are increasingly targeting third-party pathways as a potential weak link in an organization's defenses. In 2023, the MOVEit breach affected multiple Asian banks and service providers due to a vulnerability in a widely used file transfer tool managed by a third-party vendor.

These supply chain attacks demonstrate the significant damage a compromised vendor can inflict. Even firms with strong internal security can be undermined by insecure partners. A "trust but verify" model is no longer enough—firms must adopt zero-trust principles when evaluating vendor access, controls, and contingency plans.

11. https://cybersecurityasia.net/managing-fourth-party-risks/#:~:text=financial%2C%20operational%2C%20and%20reputational%20consequences,processes%2C%20and%20the%20right%20tools
12. https://www.rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1470


### Geopolitical Risks Reshaping Vendor Relationships

Geopolitics has moved from a background concern to a central pillar of supply chain planning. Initiatives like the “China+1” strategy, which encourages companies to diversify operations away from China, reflect growing concerns about trade restrictions, data localization laws, and regional instability.

While geographic diversification may reduce concentration risk, it also introduces new uncertainties. Onboarding vendors in unfamiliar jurisdictions brings different legal frameworks, risk profiles, and operational challenges.

### Social Media and Instant Reputational Risk

The rise of social media means reputational damage can unfold in real time. Today, any vendor failure—from service outages to data leaks—can become a public crisis within minutes. What might once have remained a low-profile operational issue can quickly trend on platforms like WeChat, LinkedIn, Facebook, or local equivalents, putting immense pressure on client organizations to respond immediately.

# Building a Future-ready TPRM Framework

Institutions must adopt a lifecycle-centric model grounded in real-time intelligence, integrated assurance, and regulatory resilience to future-proof third-party risk management. A mature framework is built on four interlocking components:

## Lifecycle-Driven Monitoring and Risk Detection

Continuous monitoring must become the operational core of third-party oversight. While due diligence and periodic recertification remain essential, they represent fixed points in relationships that are anything but static. Material risk events—including changes to service scope, subcontracting chains, key personnel, or even internal strategy—often occur between these touchpoints and cannot be retroactively mitigated.

Effective frameworks embed persistent monitoring mechanisms to detect both internal and external risk triggers, including:

- Integration with supplier performance and SLAs
- Real-time feed ingestion (e.g., financial health, litigation, regulatory actions)
- Automated alerts tied to risk thresholds or contractual obligations
- Feedback loops from operational incidents and near misses

## Codified and Scalable Control Architecture

A technically mature TPRM function begins with a well-defined control framework, codified into policy, embedded in governance, and operationalized through process. The framework should address:

- **Outsourcing governance** (roles, escalation paths, policy ownership)
- **Risk and materiality assessments**, aligned with regulatory definitions (e.g., critical versus non-critical functions)
- **Due diligence and pre-contract evaluation**
- **Contractual control clauses**, especially around data protection, subcontracting, and business continuity
- **Ongoing oversight and monitoring**, with evidence-based recertification

Frameworks should be modular and scalable, capable of being applied proportionately across banks, insurers, and other financial institutions, while still satisfying the highest common regulatory standards.

## Materiality-Driven Segmentation and Risk Proportionality

A one-size-fits-all approach to third-party oversight is inefficient and out of step with regulatory expectations. Institutions should stratify third-party relationships based on a consistent materiality methodology, factoring in service criticality, data sensitivity, concentration risk, and substitutability.

This enables proportional oversight: higher-risk vendors (e.g., those supporting core banking platforms or handling regulated data) warrant deeper due diligence, enhanced monitoring, and more robust contractual obligations. Lower-risk vendors may be subject to streamlined oversight, improving operational efficiency without compromising control.

## Integrated Risk Management

Risk ownership is often dispersed across compliance, legal, information security, procurement, and operational risk teams in large and complex institutions. This fragmentation creates inconsistencies, redundancies, and a sense of assurance fatigue among internal and external stakeholders.

A mature TPRM model leverages integrated risk management to harmonize these silos. This entails:

- Shared risk taxonomy and control libraries
- Centralized third-party risk registers with audit-ready traceability
- Defined assurance roles, escalation thresholds, and reporting lines
- Unified reporting dashboards for Board, regulatory, and executive visibility

## TPRM with a Strategic Lens

Third-party risk management isn't about avoiding outsourcing—it's about managing it intelligently. The prevalence of guidance over prescriptive regulation in Asia is a feature, not a flaw; it reflects a regulatory intent to encourage innovation while acknowledging the real and growing risks. The challenge for firms is to move fast, but safely. With the right tools and technologies, TPRM can be significantly streamlined. Institutions that approach outsourcing as a strategic risk, rather than a tactical procurement task, will be better positioned to navigate volatility, meet regulatory expectations, and build lasting resilience.

## SAI360's unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk and compliance spectrum.

**Risk Management Solutions**

- Risk & Compliance Management Solutions
- Enterprise & Operational Risk Management
- Regulatory Compliance
- Policy Management
- Third-Party / Vendor Risk Management
- Internal Controls
- Internal Audit
- Incident Management
- Conflicts of Interest (COI)
- Gifts and Hospitality
- IT & Cybersecurity
- Business Continuity Management
- Ethics & Compliance Learning Solutions
  - Anti-Bribery & Anti-Corruption
  - Competition & Anti-Trust
  - Conflicts of Interest
  - Data Protection & Privacy
  - Exports, Imports & Trade Compliance
  - Harassment & Discrimination


SAI360 is giving companies a new perspective on risk management. By integrating ethics, governance, risk, and compliance within a single platform, SAI360 helps companies broader their risk horizon so they can manage risk from every angle.
Visit sai360.com to learn more.

206100 0625