Managing Third Party Risks in the Financial Services Industry

Date : 19 July 2023
Time : 10:00am to 11:20am (BKK Time)

With us today

Florian Magin
Financial Services Advisory

Gavin Rosettenstein
Third Party Risk

Arpit Aggarwal
Service Now Platform Architect

Natchaon Sunthonlap
Financial Services Advisory

Zeynep Turesin Soylu
Third Party Risk

Titan Thiranattawat
Financial Services Advisory

Key themes from the global TPRM Outlook Survey 2022

Third-party incidents are disrupting the business and damaging reputation

- Third parties are causing disruption and value loss
- No contractual arrangement or direct relationship with fourth parties

Businesses underestimate the need for a sound TPRM program, resulting in insufficient budgets

- Operational resilience needs more third-party risk management (TPRM)
- leadership underestimates the complexity of enabling TPRM across the enterprise

Technology is not yet fulfilling its promise

- Perfection is out of reach
- Lack of visibility into the different stages of the contracting process, all the way through to understanding which controls are in place within the third party's environment to manage service delivery in line with expectations

The challenge of limited resources is here to stay

- Many businesses do not have all the TPRM capabilities they require
- Organisations are under-resourced to effectively manage third-party risk

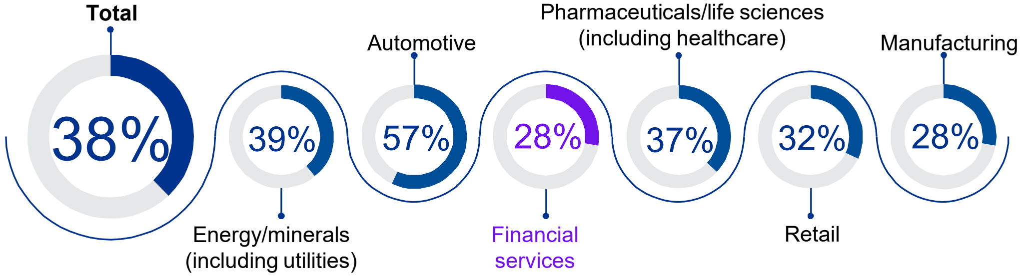
Most businesses struggle to maintain a fit-for-purpose TPRM operating model

- Organisations recognise the need to upgrade their operating model
- Many organisations have a long way to go before they achieve TPRM maturity

Source: Third-Party Risk Management Outlook 2022, KPMG International, January 2022

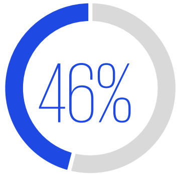
TPRM Global Outlook Survey 2022 - Results

Businesses experiencing significant disruption, monetary loss, or reputational damage as a result of a third party within the last three years

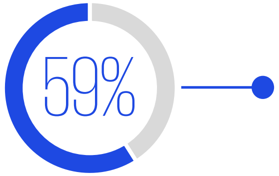


Experienced more than three incidents

Technology is not yet fulfilling its promise

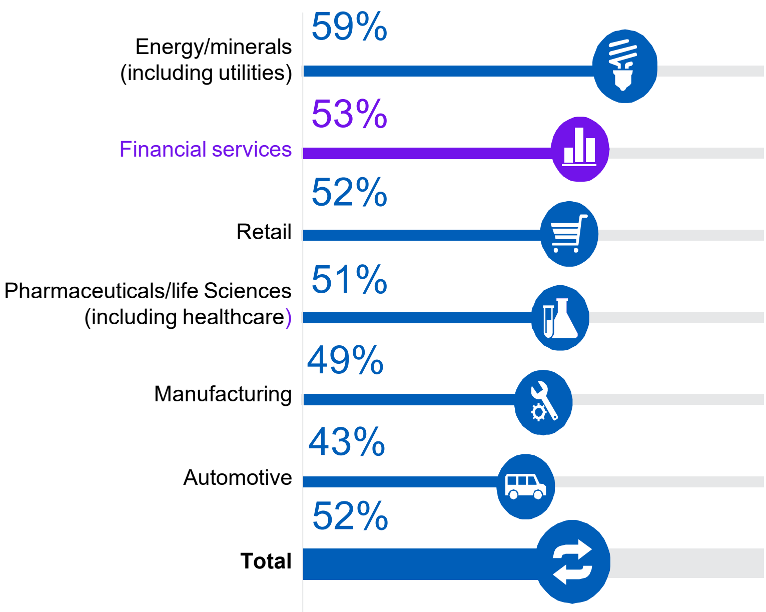


of all TPRM tasks are supported by technology or process automation



warn that their technology does not give them "anywhere near the visibility they need" to manage third-party risk across the supply chain.

Businesses without sufficient in-house capabilities to manage all the third-party risks



Source: Third-Party Risk Management Outlook 2022, KPMG International, January 2022

Key risk management drivers

There are several challenges facing organisations as they look to manage third parties and their broader supply chain.

Increased regulatory expectations

- More onerous
- Integration challenges
- Senior manager accountabilities

Poor risk management

- Risk of fines and sanctions
- Decisions not risk-based
- No single view
- Monitoring not effective / not done

Cross-organisation complex processes

- Poor end user and supplier experience
- Risk assessments taking too long
- Existing processes not unified
- No continuous monitoring
- Limited resource availability

Complex operating model

- Decentralised model
- Unclear risk ownership
- Evolving range of risk domains
- One-size-fits-all approach
- Volumes too high to manage

Technology and data

- Lack of automation
- Limited by tooling functionality
- Lack of data driven insight
- Lack of alignment and integration

Potential consequences as a result of mis-managing these challenges can result in a lack of:

✘ Speed ✘ Flexibility ✘ Visibility ✘ Consistency ✘ Depth ✘ Insight ✘ Engagement ✘ Transparency ✘ Traceability

Regulatory landscape

Areas of third-party risk

Regulatory/ Compliance Risk

- Regulatory requirements
- Theft/Crime/Dispute Risk
- Fraud, Anti-bribery and Corruption/Sanctions
- Compliance with internal procedures and standards

Strategic Risk

- Service delivery risk
- Expansion/roll-out risk
- Mergers and acquisitions
- Alignment to outsourcing strategy
- Intellectual property risk

Subcontractor Risk

- Applicable across all risk areas

Concentration Risk

- Supplier concentration across critical services
- Industry concentration (incl. subcontractor)
- Concentration of critical skills (i.e., tech support)
- Geographic concentration
- Reverse concentration

Technology/ Cyber Risk

- Information security
- Cyber security
- Data privacy/data protection

Country Risk

- Geopolitical risk
- Climate sustainability

Financial Viability

- Financial risk from lending to a third party
- Liquidity risk

Operational/Supply Chain Risk

- Business continuity
- Disaster recovery
- Physical security
- Operational Resilience
- Performance management (incl. SLA's)
- Model risk
- Human resources risks (conduct risk, etc.)

Reputational Risk

- Negative news
- Lawsuits (past and pending)
- Brand of the third party
- Key principals/owners of the third party
- Workplace safety
- ESG

Legal Risk

- Jurisdiction of law
- Terms and conditions of the contract

TPRM target operating model

Risk domains

- Geopolitical risk
- ESG risk
- Fraud risk
- Litigation risk
- Regulatory / compliance risk
- Subcontractor risk
- Technology/ cyber risk
- Financial viability
- Strategic risk
- Concentration risk
- Reputational risk
- Operational/ supply chain risk

Lifecycle phases

1. Planning & supplier identification
2. Due diligence & risk decision
3. Contract management & on-boarding
4. Ongoing monitoring
5. Off-boarding

Foundations of a TPRM program

- Policies and procedures
- Organisation, people, skills, and training
- Governance and program effectiveness
- Data and reporting processes
- Enabling technology

Insights based on TPRM implementation experience

As the industry leader, KPMG provide clients with real insights necessary to successfully implement a fit-for-purpose TPRM program.

People (Across 3LoD)

- Overclassified critical/high rated suppliers are driving increased cost of oversight by 35%
- Centralised TPRM teams can reduce workloads of relationship owners by up to 80% and decrease risk team involvement by 40-60%
- Employee resistance to change is top five reason TPRM programs don’t realise full potential

Process Pain Points

- Lack of integration between Procurement and TPRM around intake increases through put time by up to 40%
- 30-60% of TPRM processes are manual causing unnecessary operating and head count costs
- Revising risk and procurement questionnaires can lead to 30-50% reduction in overall question count

Technology Integration

- A fully integrated TPRM architecture process will reduce operating costs by 20-35%
- Central planning and intake will reduce error rates by 10-15%
- A common TPRM language eliminates up to 25% of effort over the course of a year for a top tier client across lifecycle

Risk Framework

- Critical vendors should not exceed 100 to allow for right-sized adequate oversight (dependent on industry)
- 50% of clients are planning to incorporate the “E” of ESG into TPRM in the coming 18-24 months
- 80% of our clients are working on enhancing their fourth party risk management program oversight

Data & Reporting

- Leading institutions are building next gen TPRM scoring methodologies using AI to speed up risk assessment process and better allocate TPRM resources resulting in overall reduction of scoring effort by 30-50%
- 40% of clients have suffered a disruption in BAU activities during the pandemic as a result of a supplier failure
- Approximately 75% of our clients state that technology is the primary driver for the lack of clarity in TPRM reporting across procurement, risk and the business

What does the future of TPRM look like

Third party risk management will be consistently applied across an enterprise, strengthen compliance and utilise integration across tools, ultimately reducing costs and provide time efficiencies.

Compliant & robust

- Monitor the control environment and risk profile for critical third-party products and services on a consistent basis.
- Understand correlations and relationships between third party metrics.
- Anticipate service disruptions before they occur.

Consistent across the enterprise

- Replicate TPRM outcomes across regions, businesses and risk domains.
- Holistic risk appetite and program strategy enable the program to scale across the Enterprise.
- Establish TPRM risk culture and gain business buy-in.

Cost & time efficient

- Reduce onboarding cycle times and program costs with optimised and streamlined processes, effective risk segmentation that focuses due diligence activities, and the use of managed services to augment in-house teams.

Integrated with complementary processes & tools

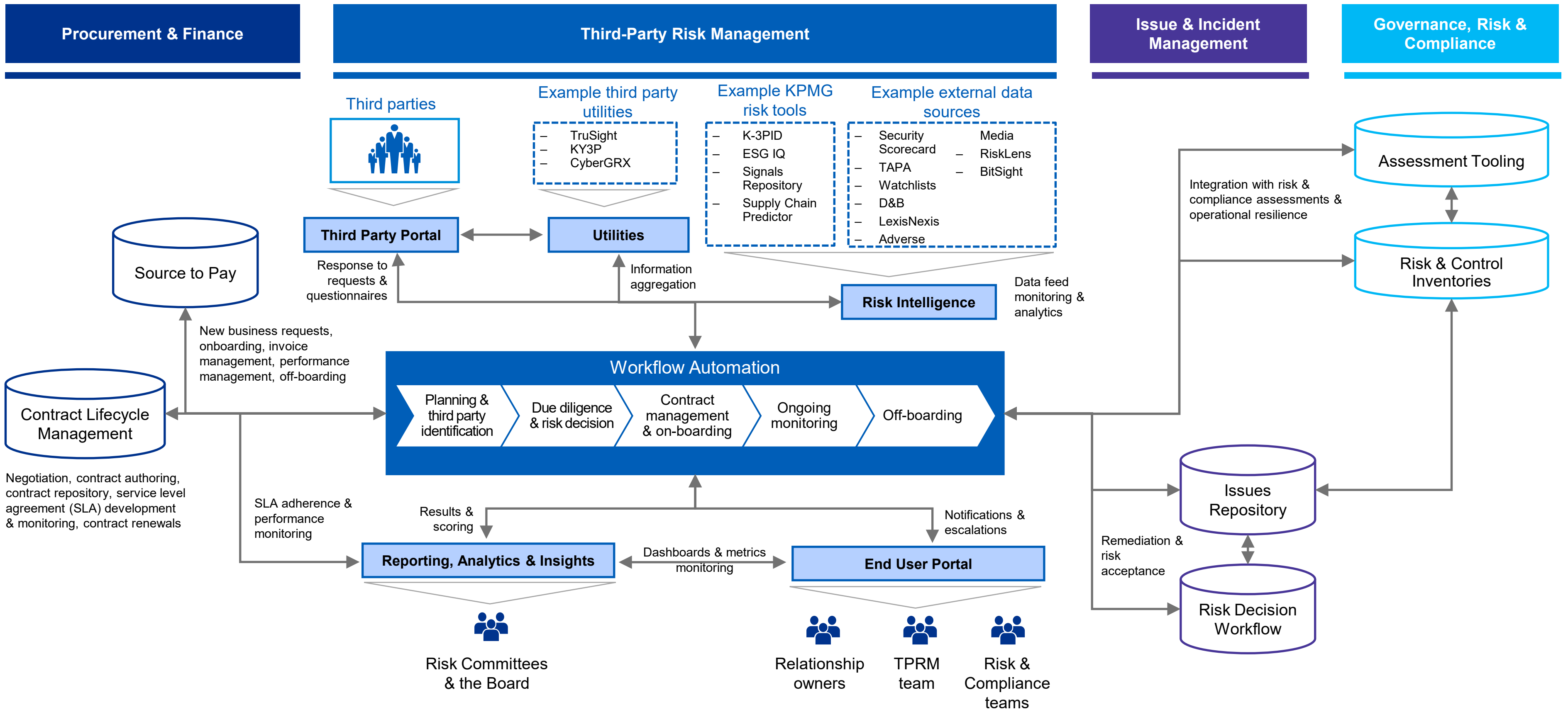
- Enhance user experience across stakeholders with a seamless TPRM process integrated with procurement and contract lifecycle management, as well as centralised issues management.
- Incorporate TPRM into enterprise assessments.

Enablers to achieve the future state

- **Data-driven approach** with a comprehensive data model and complete inventory
- **Rules-based process**, particularly scoring, escalation and ongoing monitoring approach
- **Automation** of standardised and rationalised processes
- **Use of managed services** and risk intelligence services to decrease TPRM tasks
- **Centralised** service delivery model

Powered TPRM functional architecture

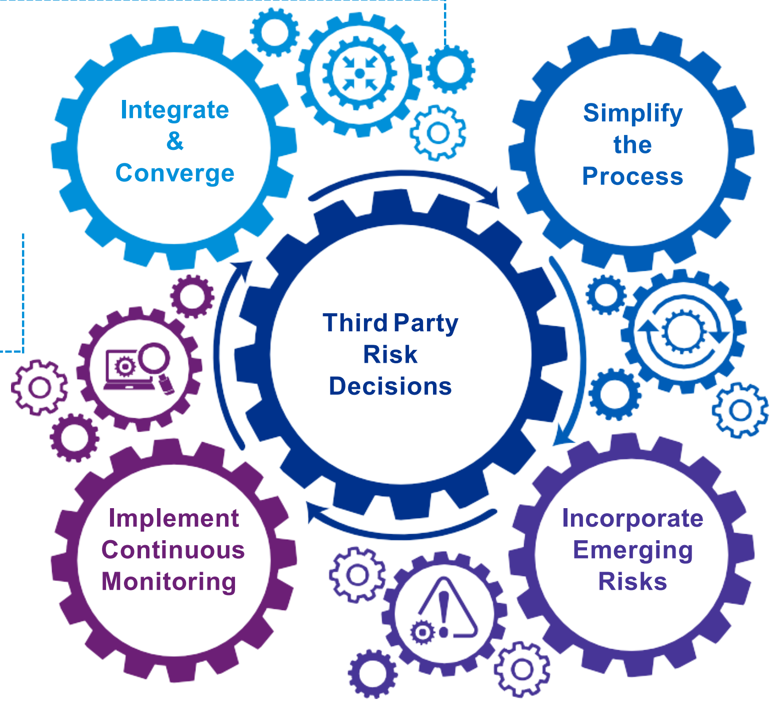
The future-state TPRM functional architecture can enable a compliant, consistent, efficient and integrated TPRM process:



Where are TPRM leaders focusing?

Integrate & Converge

- Enterprise Risk & Compliance Integration
  - Risk Appetite
  - Risk & Control Assessments
  - Testing
- Operational Resilience
- Global Regulatory Compliance & Change Management
- Affiliate Risk Management



Simplify the Process

- Service Delivery Model
- Risk Segmentation
- Workflow Technology
- Data Analytics
- Business Intelligence

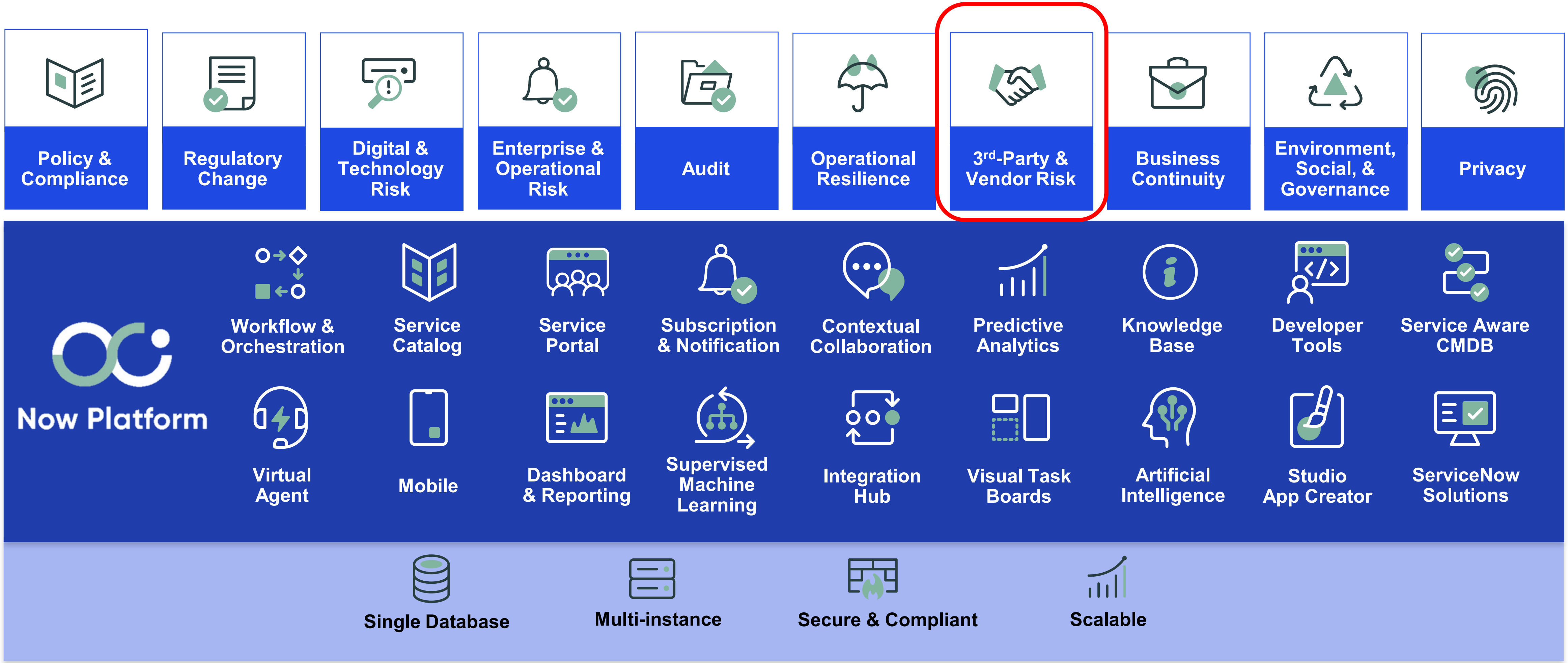
Implement Continuous Monitoring

- Risk-Based Scoping
- Internal & External Data Sources
- Data Model
- Real Time Scoring
- Escalation Protocols

Incorporate Emerging Risks

- Trend & Exception Monitoring
- Key Risk Indicators
- Risk Lens Expansion
  - Concentration Risk
  - Subcontractor Risk
  - Remote Contingent Workers
  - Environmental, Social, Governance (ESG)

A platform-based approach to TPRM



Demo

Vendor or Third-Party Risk Management

Adam Haro, Vendor Manager

Vendor Tiering & Vendor Assessment

Owen Orpen, Vendor Contact

Sales Executive –Cloud MSP

Q&A

Key takeaways

Early / Medium stages of maturity
Focus: Must-haves

Pre-Contract Due Diligence

Completion of due diligence prior to executing the contract. Depending on the industry and service, key risks such as cyber security, business continuity or compliance may be prioritised over other risks.

Risk-based approach

Consideration of limited time and resources to focus on the third-parties that impact the most critical services. As the TPRM program matures, the scope can expand to cover broader tiers of third-party arrangements as well as additional risk domains

Ongoing Monitoring

Ongoing monitoring plan to assess, over the lifetime of the contract, that the third-party is delivering in line with expectations.
The control assessment should be done by the relationship owner and overseen by a function responsible for that risk.

Program Governance

Overseeing, monitoring and governing the arrangement, effectively resolving incidents that occur, and managing occasions when a decision is required that is at odds with the stated policy.
To avoid ineffective challenge and poor decision-making, policies and clear role and responsibility definitions are required.

Automation

Organisations are looking to automate the end-to-end workflow to enable faster decision-making and assist in managing costs. To complete tasks for various components and streamline the due diligence process industry utilities or feeds can be leveraged.

Risk-based approach

Further streamlining the risk tiering of third-party services, the criteria used to delineate something as critical or high risk.

Advanced stage of maturity
Focus: Optimising Program

Off-boarding & disengagement

How to exit a relationship while service continues to be delivered to customers and markets.
Mapping specific services to products & processes within the organisation is critical.

Service Delivery Model

A unified, enterprise-wide "center of excellence"
The center of excellence is one of the most efficient ways for organisations with limited resources to cover the broad population of third-parties.

Management of fourth parties & affiliates

In mature programs, fourth parties, intercompany and intracompany transactions – are no longer out of scope. Appropriate controls such as contract documentation and aligning program steps with TPRM program requirements can be beneficial to the organisations.

QR Code for Feedback

kpmg.com/th

Twitter: @KPMG_TH
LinkedIn: linkedin.com/company/kpmg-thailand
Facebook: facebook.com/KPMGinThailand
YouTube: youtube.com/kpmginthailand
Instagram: instagram.com/kpmgthailand