

Third parties: Changing risks and the role of internal audit

Craig Wright

15 September 2021

Agenda

Introduction to Third Party Risk Management (TPRM)

Changing TPRM landscape

Internal Audit review of TPRM

Q&A



Introduction to Third Party Risk Management ('TPRM')



Who are third parties?



How?

- On-shore
- Off-shore
- On-site
- Off-site
- Integrated
- Cloud
- Ongoing relationship
- One-time purchase



What?

- Trade reporting
- Call centre
- Advertising
- Printing statements
- Back office functions
- Referral relationships
- Software
- Data warehouse
- Trading platform



Who?

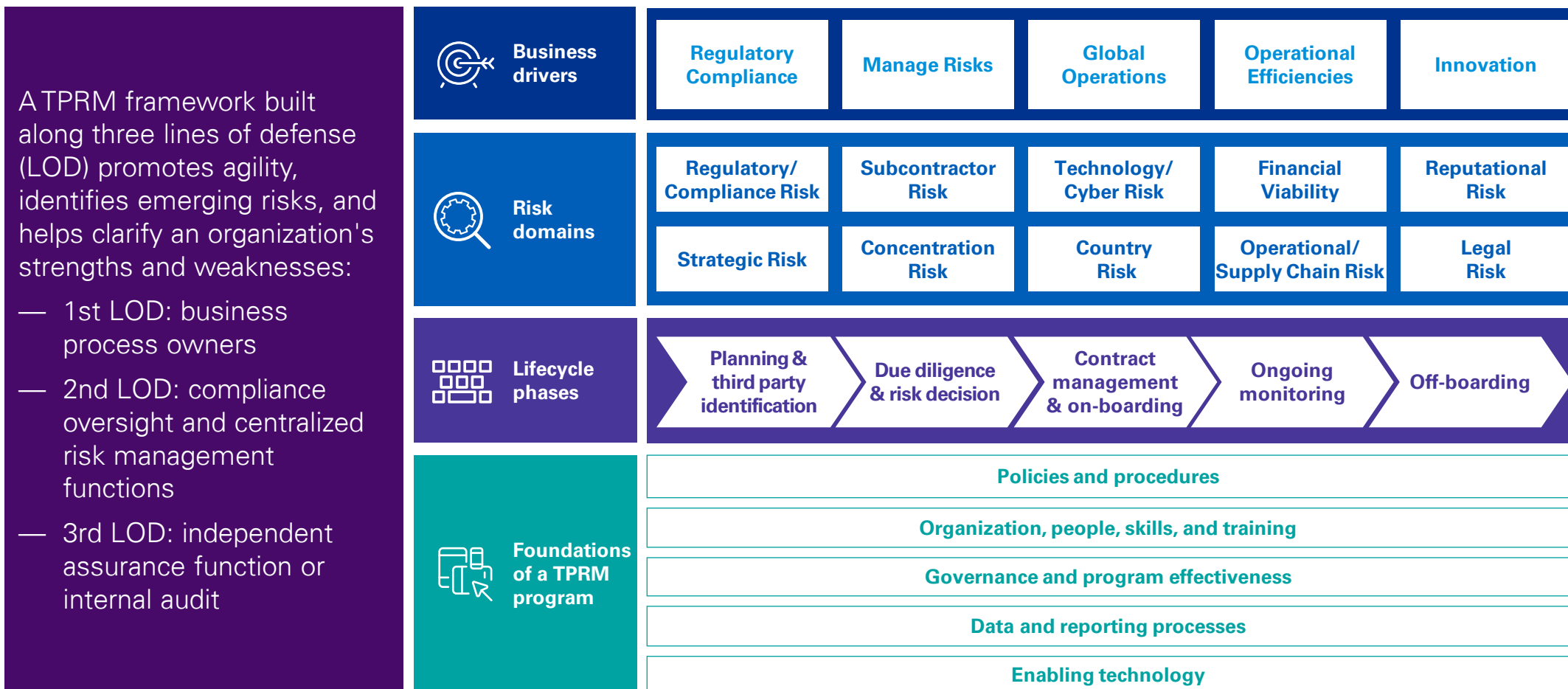
Internal

- Affiliates
- Shared Services
- Legal entities

External

- Alliances
- Partnerships
- Vendors
- Joint ventures
- Suppliers
- Contingent workers
- Outsourced providers
- Contingent deals

Three lines of defense TPRM operating model





Changing TPRM landscape



Key issues facing clients

5. Technology and data

- Processes overly manual
- Current tools have limited functionality, not proactively driving risk management
- Industry utilities and data feeds not being leveraged
- Lack of alignment and integration with Procurement, Risk, Business, Functions
- Few insights and lack of analytics, no predictive capability

4. Process

- Poor end user and supplier experience
- Risk assessments taking too long, inefficient process
- Existing processes not unified, do not meet business and regulatory expectations
- No continuous monitoring – point in time approach
- Limited resource availability and capability

1. Increased regulatory expectations – UK, Europe, Global

- More onerous – higher expectations, wider scope on outsourcing, third parties and cloud
- Integration challenge – how does this link to Operational Resilience and ERM
- Senior Manager accountabilities

2. Increasing reliance, poor risk management

- Digital partnerships / alliances / move to the cloud is growing
- Decisions not risk-based, processes not agile
- No single view of third party risk
- Monitoring not effective / not done – risks outside of appetite
- Inappropriate / insufficient levels of due diligence, risk not managed over the term of the relationship / engagement
- Expensive but not generating value

3. Complex operating model

- Decentralised model brings inconsistency in risk decisions and oversight
- Risk ownership unclear and framework outmoded
- Evolving range of risk domains – eg ESG
- One-size-fits-all, not sufficiently risk-based, not intelligence-led
- Volumes too high to manage



Where are TPRM leaders focusing in the new reality?

Programs are building on the lessons learned from COVID-19, in order to increase their ability to enable confident, informed third-party risk decisions.

Integrate & Converge

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

Implement Continuous Monitoring

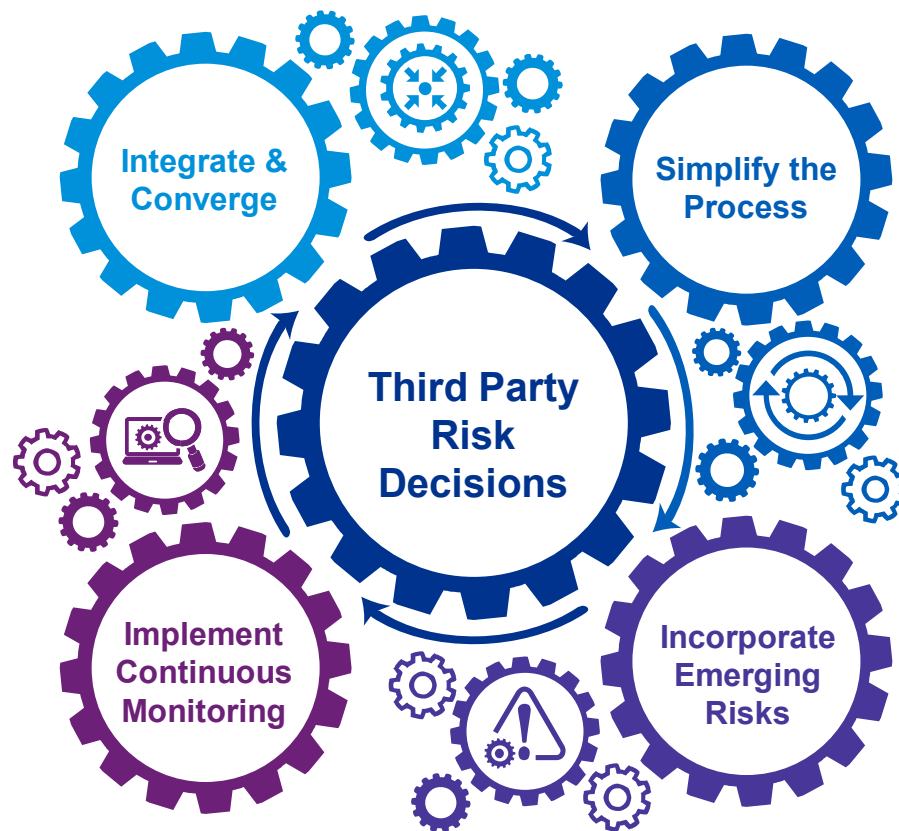
- Risk-Based Scoping
- Internal & External Data Sources
- Data Model
- Real Time Scoring
- Escalation Protocols

Simplify the Process

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

Incorporate Emerging Risks

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



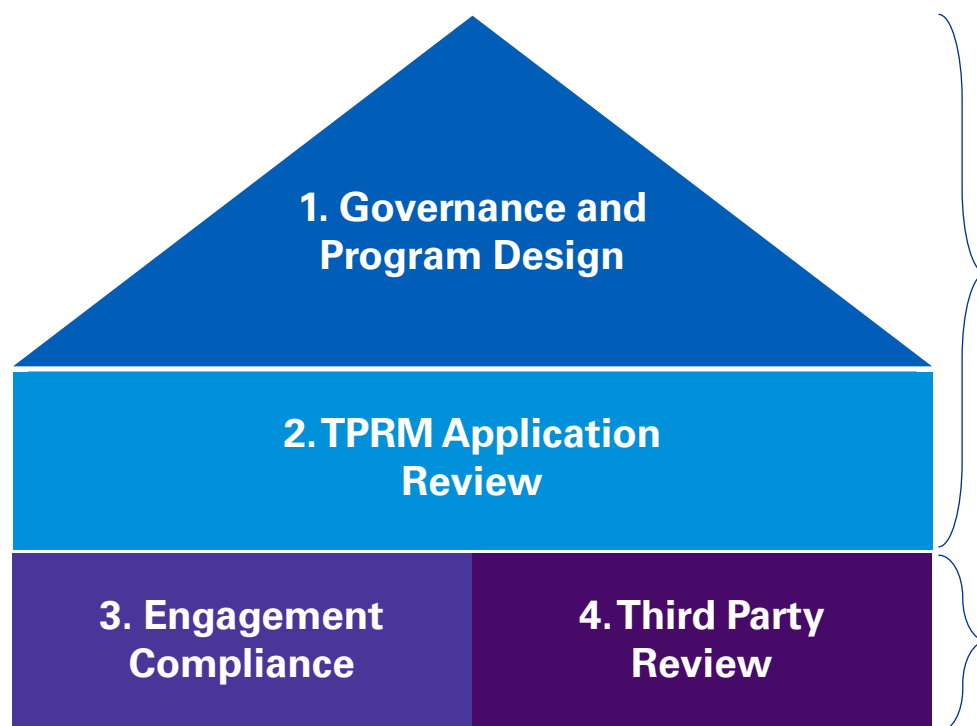


Internal audit review of TPRM



TPRM internal audit framework

Internal Audit can focus on four inter-related components to analyze both design and effectiveness across the TPRM lifecycle: (1) Governance and Program Design, (2) TPRM Application Review, (3) Engagement Compliance, and (4) Third Party Review.



Program level audits

1. Governance and Program Design: Evaluate program level aspects such as Board and senior management oversight, alignment with regulatory expectations and enterprise-wide risk management programs, as well as assessing the comprehensiveness of program coverage across affiliated and non-affiliated third parties

2. TPRM Application Review: Assess technology enablement features including triggers, access controls, data reporting across the organization, and integration with Risk Management and Procurement technology

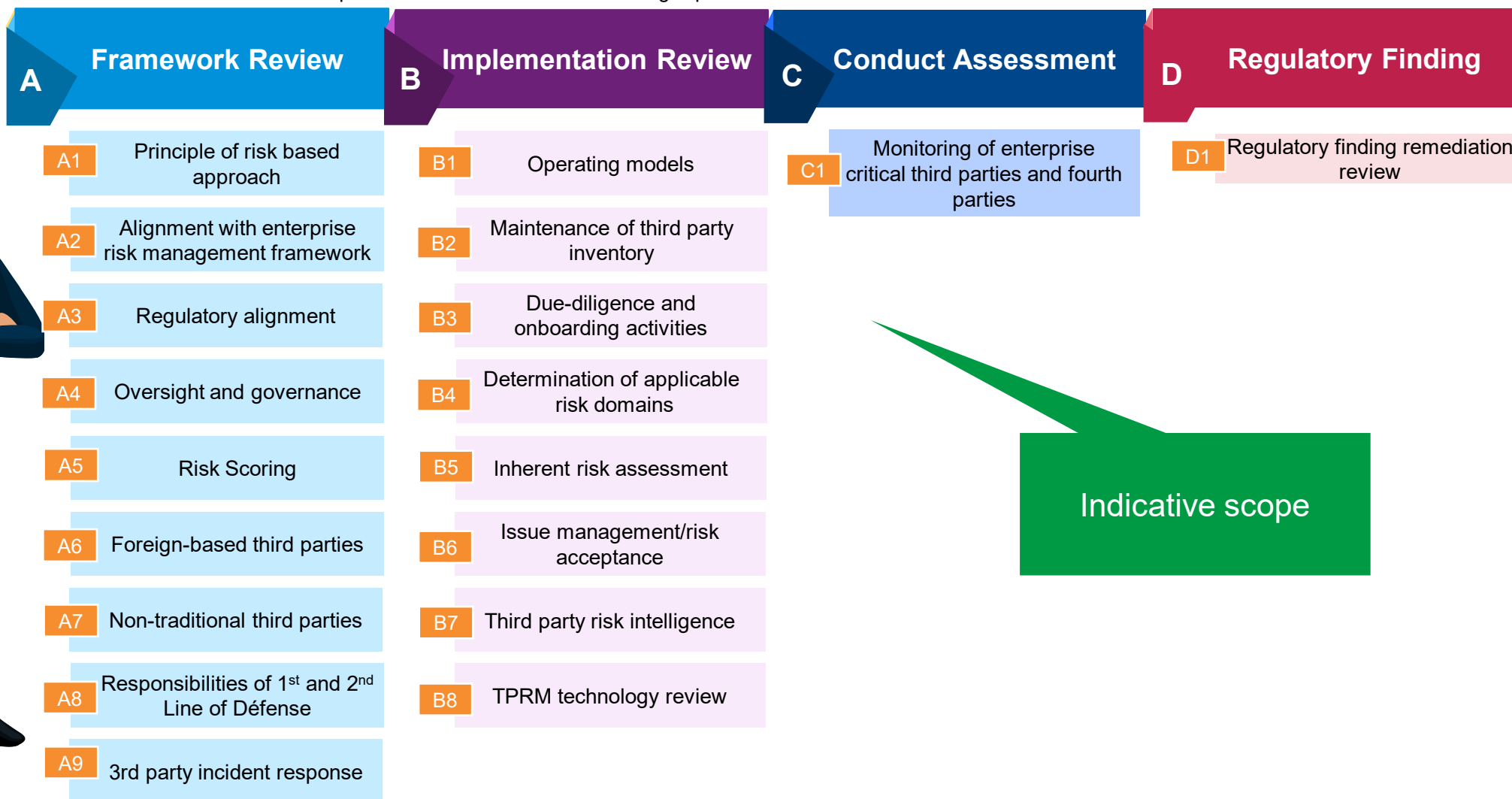
Engagement level audits

3. Engagement Compliance: Evaluate business adherence to pre-contracting and post-contracting requirements as specified in the TPRM policies and procedures





4. Third Party Review: Evaluate third party and engagement-specific controls through desktop and on-site reviews

TPRM Audit Scope Areas

The internal audit function could scope in TPRM in either/ all the following capacities.



Key Considerations for Auditing Third Parties Across the Lifecycle

 Planning and third party identification	 Due diligence and risk decision	 Contract management and on-boarding	 Ongoing monitoring	 Off-boarding
<ul style="list-style-type: none"> — Is there a complete list of third parties available? — Is the risk profiling completed at arrangement level or third-party level? — Is inherent risk assessed across all applicable risk domains? — How do you ensure that inherent risk is correctly assessed? — Is inherent risk revisited periodically? 	<ul style="list-style-type: none"> — Is a risk-based approach to due diligence implemented? — How do you ensure that due diligence covers all applicable risk domains? — How are issues identified as part of due diligence addressed? 	<ul style="list-style-type: none"> — Is there a standard list of terms and conditions per applicable third party and per third party service type? — For cases, where third party terms and conditions are leveraged as basis, how is contract risk assessed? — Is there a risk-based exception approval process defined for deviations from standard contract? — Is the contract reviewed periodically to assess compliance to any organization/ regulatory obligations? 	<ul style="list-style-type: none"> — How is the risk profile for third party arrangement kept up to date? — Does the risk profile take into consideration inputs outside periodic assessments (incidents/ internal audit/ risk intelligence etc.)? — How is business unit driving issue remediation for any observations identified? — Is a risk-based approach to ongoing monitoring? — What is the process in place to make sure the ongoing monitoring approach complies with all applicable organization policies and regulatory obligations? — How do you ensure that ongoing monitoring covers all applicable risk domains? 	<ul style="list-style-type: none"> — Following a risk-based approach, is there a defined contingency plan for third parties? — How are transition risks addressed? — How do you ensure compliance with data security requirements for termination? — How do you address IP related risks in event of arrangement termination?



Craig Wright

Governance, Risk and
Compliance Services

Craig.Wright@kpmg.co.uk





kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.