Operationalising third-party risk management

A broad array of risk domains can be customised to meet requirements.

Risk domains

Data privacy/infosec/ cybersecurity
Fails to comply with organisation and/or legal/regulatory standards for the management and protection of your organisation's personal and/or sensitive data

Concentration risk
Contracted exclusively to perform critical/high-risk functions exposing your organisation to overreliance on a single organisation for service provision

Environmental impact and health and safety
Does not comply with an organisation's standards for workplace health and safety, and delivers goods or services in a manner that causes harm to employees or customers or environment

Fourth-party/sub-contractor risk
Involves the risk of a fourth party or sub-contractor with inadequate internal operational and information security controls; this could expose the client organisation to supply chain risk, resulting in reputational, regulatory, legal and/or operational risk

Performance management and contract compliance
Adheres to contractual requirements, defined SLAs, industry standards and requirements, regulatory guidelines, etc.; compliance to key contract clauses

Business continuity/ resilience
A failure to supply goods or services due to the inability to adequately manage a disruptive event in their supply chain, resulting in an adverse impact on the organisation

Conduct/ethics
Provides goods or services on the organisation's behalf that leads to customer detriment or has an adverse impact on market stability or effective competition; additionally, background of promoters and key management personnel

Geopolitical
Is in a geography that is exposed to political or economic instability, which could expose the client organisation to supply chain risk in the form of a natural disaster or political event

Regulatory compliance, including sanctions and exports
Provides goods or services in a manner that is not compliant with local and national regulations, international sanctions, and export control regulations, exposing your organisation to reputational risk or fines

Labour rights
Uses unethical labour practices, such as child labour, forced labour, discrimination, and unfair pay, to deliver goods or services; this results in reputational, regulatory, legal and/or operational risk

Financial health
Is no longer financially viable and therefore, unable to deliver a stable service or product, resulting in operational risk

Deloitte.

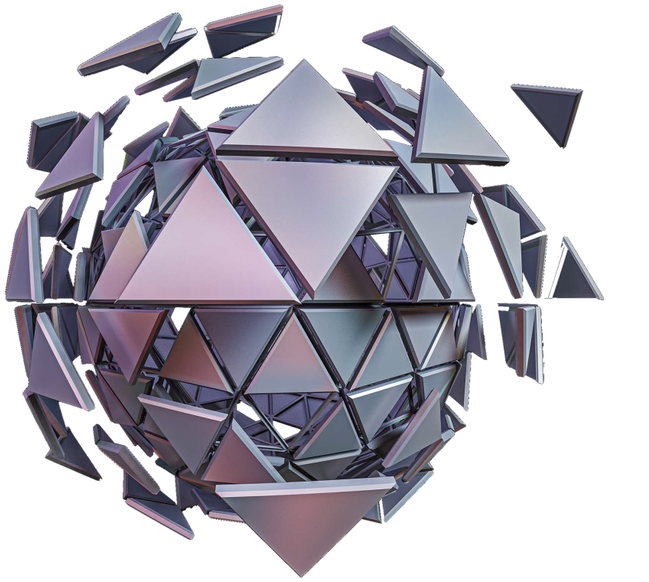
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.

© 2022 Deloitte Touche Tohmatsu India LLP. Member of Deloitte Touche Tohmatsu Limited

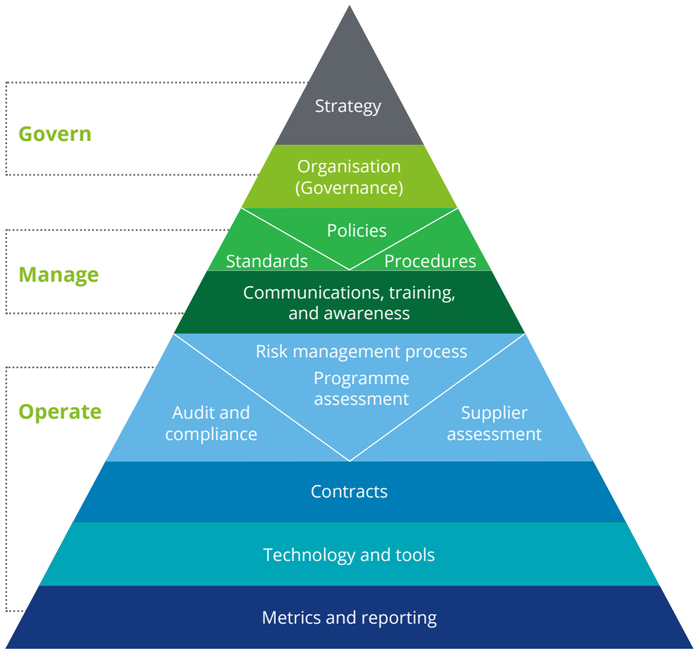
Deloitte.



Governing and operationalising third party risk management

April 2022

Governance of third parties



A formal strategy defining the role of the TPRM programme within the enterprise VRM function to ensure a single view of third-party risk to the organisation

Well-defined roles and responsibilities to develop an optimised organisational structure to manage the third-party assessment lifecycle, including termination activities

Policies, standards, and procedures defining risk assessment methodology and activities, risk tolerance levels, and integration points with other third parties and risk management functions to ensure consistency and quality in programme activities

Coordinated communication channel to inform stakeholders of the TPRM and the programme's business value programmes to educate stakeholders of responsibilities at each stage of the TPRM lifecycle

Formal processes to assess the effectiveness of the TPRM programme against programme and organisational requirements

Contracts to act as legally binding agreements that recognise and govern the rights and duties of the parties to the agreement

Tools and technology driving groups to use common risk management processes that enhances the effectiveness and efficiency of the TPRM programme

Metrics and reporting requirements for risk assessment activities and programme operational components to ensure data quality, and accuracy and audience-specific reporting

Operationalising third-party risk management

Policy, procedures, standards, and guidelines

Data sources (company internal systems, such as ERP, CRM, and billing system)

New/existing third parties

- Third-party evaluation
- Third-party selection
- Contract and onboard
- Termination

Third-party prioritisation

- Parameters/third-party information → • Spend • Services • Others
- Risk engine → • Confidentiality • Integrity • Availability
- Third-party profile → • Service Categorisation • Inherent risk profile
- Third-party coverage model → • Review method • Frequency • Review type • Reporting

Domains

- Labour rights
- Financial health
- Fourth-party risk
- Concentration risk
- Data privacy, info sec and cyber security
- Regulatory compliance
- Environmental impact, health, and safety
- Business continuity and resiliency
- Performance management and contract compliance
- Conduct/ethics
- Geopolitical

Review method

- Self assessment
- Onsite
- Remote
- Continuous monitoring
- Hybrid

Manage, monitor and remediate

Reporting

- CISO team
- Chief risk office
- Supply chain
- Business controller

Key Performance Indicators (KPI)

Enablers - Automation

- Views
- Workflow
- Data repository
- Analytics and reporting

Review coverage

- Review of business controls
- Review of both business and information security controls
- Review of information security controls