Understanding and Securing Third-Party and Supply Chain Risks

As businesses increasingly depend on external entities for a diverse range of offerings such as IT services, marketing, logistics, and finance, engaging with third parties alters the organisations risk landscape. This exposes organisations to similar risks faced by service providers, encompassing operational, compliance, legal, financial, and reputational concerns. An organisations risk posture, therefore, must align with that of their service providers, extending to potential issues related to inadequate due diligence, vulnerabilities in the supply chain, data breaches, cyber-attacks, and other security threats.

While many organisations have well-developed capabilities in identifying, assessing, and mitigating risks more broadly, including cyber capabilities and protection of information assets, there is still work to do.

Recently, ASIC Chair Joe Longo said…

> *'For all organisations, cyber security and cyber resilience must be a top priority. ASIC expects this to include oversight of cyber security risk throughout the organisation's supply chain – it was alarming that* ***44% of participants are not managing third-party or supply chain risks****. Third-party relationships provide threat actors with easy access to an organisation's systems and networks.'*

By establishing and maintaining strong preventative and reactive TPRM practices, organisations can ensure ***third-party, and supply chain*** risks are, identified and assessed early and continuously, improving third-party relationships, and enhancing an organisations resilience and risk profile.

What is Third Party Risk Management (TPRM)?

TPRM stands for Third-Party Risk Management and refers to the process of **identifying**, **assessing**, and **mitigating** risks associated with third-party vendors, suppliers, and service providers that an organisation relies on to conduct its business operations. Also known as Vendor Risk Management (VRM), TPRM goes beyond the general risk management and Governance, Risk and Compliance (GRC) principles by integrating both preventative and reactive measures into vendor management practices, enhancing an organisations resilience to potential disruptions and minimising the impact of unforeseen events. A comprehensive approach involves ongoing monitoring, collaboration with suppliers, and a commitment to continuous improvement.

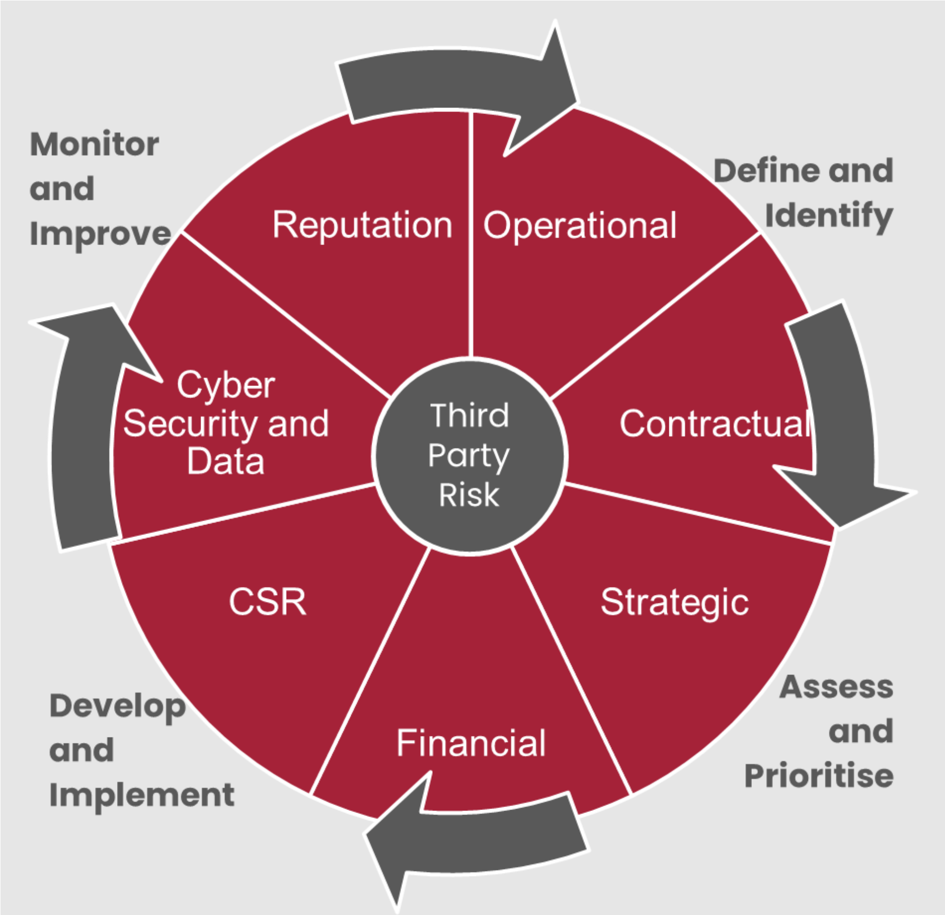
Preventative Supplier Risk Management enables the early detection and response to potential disruptions, delays and risks that threaten operations, ensuring supply chain trust, integrity and resilience, ensuring vendors deliver as per agreement or expectations. **Reactive Supplier Risk Management** enables effective monitoring of Third-Party performance and compliance with contractual obligations, ensuring Supplier Risk Management controls and risk mitigation strategies are effective enabling measured response to underperformance and/or supplier incidents, ensuring supply chain trust, integrity and resilience.

Why Identify, Assess and Mitigate Third Party Risk?

It is important for organisations to **identify**, **assess** and **prioritise** the following risks by understanding and implementing appropriate **risk mitigation strategies**. By establishing strong contractual agreements, and regular and consistent monitoring and assessment, organisations can ensure third-party relationships are managed effectively:

- **Operational Risk**: Monitor regulatory compliance, the effect of a vendor failure, technical and physical security risks, aged assets, insurance coverage, OH&S and associated fraud risks.
- **Contractual Risk**: Contractual exposure including Vendor capacity, end of life or inability to enforce the contract.
- **Strategic Risk**: Inconsistency in strategic direction and the level of management needed, and inadequate expertise and risks associated with outsourced or offshore operations.
- **Financial Risk**: Assessment of the potential for financial failure, assessed at onboarding and monitoring of financial strength.
- **Corporate Social Responsibility**: Onboarding assessment and annual assessment covering Environment, Labour and Human Rights (inc. Modern Slavery), Ethics and Sustainability.
- **Cyber Security and Data Governance**: Assessment of data housed with Vendors, where it is hosted, and physical site security inspections.
- **Reputational Risk**: Review negative news and media associated with poor service, disruptions & impact on client or the client's customers.

Effective TPRM can help an organisation manage risks associated with the access to and the use of information assets, and the use, support, and management of IT infrastructure, by implementing appropriate risk management strategies and controls.


Monitor and Improve
Define and Identify
Assess and Prioritise
Develop and Implement
Reputation
Operational
Contractual
Strategic
Financial
CSR
Cyber Security and Data
Third Party Risk

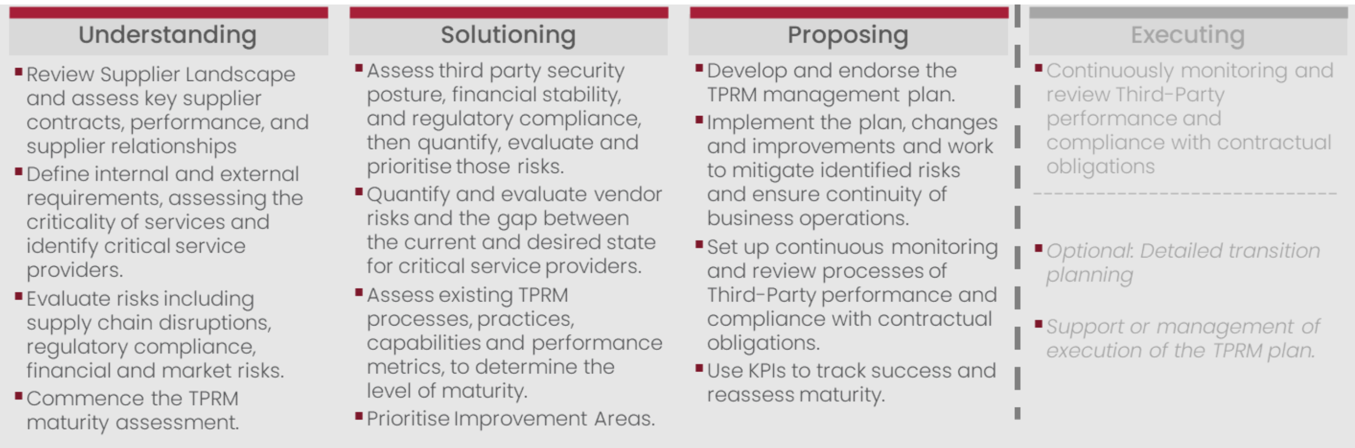
Why it Matters

- Supplier due diligence during the RFP process and/or at on-boarding indicates the **integrity** and **resilience** of new suppliers and drives decisions regarding engagement and contractual risk mitigation.
- Carrying out supplier tiering, and analysis of Critical Service Providers (CSPs), in line with the Security of Critical Infrastructure Act 2018 (SOCI Act) *, based on criteria of business **criticality**, **risk level** and **spend value**, drives prioritisation of contracts and performance management, informing the governance process, the management of tasks and frequency at which they occur.
- Ongoing **third-party monitoring** of financial performance, company structure and any fraudulent activity, adverse legal proceedings, insolvency actions and defaults enables the early detection of potential disruptions, delays and risks.
- **Monitoring of compliance** to obligations under the Contract such as compliance with any applicable GRC (Governance, Risk and Compliance) and ESG (Environment, Social and Governance) regulations and standards including human rights obligations consistent with the **Modern Slavery Act 2018** further mitigates adverse risk in the supply chain.

CDRU Support

The CDRU unique Strategic Sourcing Framework "USP" (Understanding; Solutioning; Proposing) methodology covers the analysis, solutioning and then proposing recommendations and an implementation plan to apply the recommended changes and improvements. Our approach outlines clear and practical steps to define and identify an organisations critical processes, outline internal and external requirements to then identify and mitigate supplier risks.

CDRU's USP process comprises the following stages and activities:



Understanding	Solutioning	Proposing	Executing
Review Supplier Landscape and assess key supplier contracts, performance, and supplier relationships Define internal and external requirements, assessing the criticality of services and identify critical service providers. Evaluate risks including supply chain disruptions, regulatory compliance, financial and market risks. Commence the TPRM maturity assessment.	Assess third party security posture, financial stability, and regulatory compliance, then quantify, evaluate and prioritise those risks. Quantify and evaluate vendor risks and the gap between the current and desired state for critical service providers. Assess existing TPRM processes, practices, capabilities and performance metrics, to determine the level of maturity. Prioritise Improvement Areas.	Develop and endorse the TPRM management plan. Implement the plan, changes and improvements and work to mitigate identified risks and ensure continuity of business operations. Set up continuous monitoring and review processes of Third-Party performance and compliance with contractual obligations. Use KPIs to track success and reassess maturity.	Continuously monitoring and review Third-Party performance and compliance with contractual obligations *Optional: Detailed transition planning* *Support or management of execution of the TPRM plan.*

To uncover how CDRU can use their strategic sourcing expertise to achieve your organisations optimisation goals, get in touch now.

References:

- ASIC calls for greater organisational vigilance to combat cyber threats, Published 13 November 2023: https://asic.gov.au/about-asic/news-centre/find-a-media-release/2023-releases/23-300mr-asic-calls-for-greater-organisational-vigilance-to-combat-cyber-threats/.
- The Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP Act) came into effect on 2 April 2022.