Vendor Risk Management

Third Party Risks in a Vendor management are:

- **Loss of reputation –** Risk to the reputation of the organization from the use of third-party relationships due to a myriad of reasons including misuse of intellectual property; poor product quality; lack of compliance to human rights and environmental regulations, etc.
- **Supply chain disruption –** Key third party business disruption due to bankruptcy, geopolitical issues, macro risks etc. can result in supply chain disruption
- **Data risk –** Loss, misuse or mishandling of critical data of the organization or its customers by a third-party relationship can result in financial loss; hefty fines and decrease in shareholder value
- **Product recall –** Poor product quality, safety issues or faulty packaging by third parties can lead to product recalls resulting in recall costs, lawsuits from consumers, increased costs from settlements, and lost revenue from missed sales opportunities.
- **Financial impact –** Financial loss from under-reporting of revenue from licensees, royalty partners, distributors, franchisees etc. and over-payments for services from third party relationships

- **Lack of compliance –** Third party acts corruptly to gain business advantage for organization resulting in hefty fines or is not in compliance to Environment, Conflict Minerals, Health and Safety, Labor Rights etc. regulations.
- **Poor Performance –** Lack of sustained performance from third party relationships resulting in costly mistakes, over allocation of capital to oversee relationship and defeating the purpose of outsourcing strategy

Sectoral insights and point of view: By deploying an end-to-end VRM solution for 'all things Risk', across variegated industries, we can identify sectoral pain points and attain differentiated insights in comparison to publicly available information. Some of the over-arching challenges from the across sectors are listed below:

Pharmaceuticals and Lifesciences (LS):

- Geopolitical risks due to changing political landscapes and unions, etc.
- Lack of quality and safety controls/measures by third parties in manufacturing and supply chain management. Parent companies capable of non-compliance to regulations such as FCPA in the US and the Bribery Act in the UK.

Healthcare (HC):

- Once information is in the hands of business associates and subcontractors, covered entities tend to lose track of where it is and how it's being used.
- Business associates are notorious for security leaks. Some business associates are unaware of their status and potential gaps (be it cyber, financial, strategic, etc.). Sound risk management practices are required to ensure user organisations are able to monitor their partners.
- Industry undergoing changes in risk management approach. Processes will be risk-based more than 'compliance-based' to best protect customers, and not just align privacy and security with regulations

Automotive

- Auto sector undergoing changes in the nature for the risks involved. For example, business interruption risks are moving from tangible ones to virtual forms.

- Imbibing a culture that is risk-agile and ensuring employees are prepared with the necessary skills to ensure that compliance efforts keep pace with innovation and growth
- Understanding of cyber security required, including implications of data that is collected and how it should be shared, managed, and stored, particularly when forming of new partnerships and joint ventures.

Technology (IT/ITES)

- Absence of Customer SLA / claim/ payment term back to back arrangement with vendors.
- SLA, licensing, attendance and contractual monitoring for outsourced on-shore delivery and sub-contracted (4th parties).
- Huge dependency on cloud delivery platforms and usage of IP and associated cost.
- Stringent and dynamic government regulations (EU GDPR, HITRUST, FINRA, SOX, etc.)

Insurance

- Over/ Under Underwriting & Inadequate reinsurance
- CRM for Policy issuance and claim management
- Huge dependency on cloud delivery platforms and usage of IP
- Stringent and dynamic government regulations (EU GDPR, HITRUST, IRDA, SOX, etc.)

Payment Cards (PC):

- The scope of fraud, misuse, and lack of security are slowly becoming the most common risks associated with third-party payment processors.
- Cyber frauds increasing at an alarming rate
- Lack of clarity and monitoring of third party triggered illicit activities can cause identity thefts via using a persons' PII without their permission, to commit fraud or other crimes.

Banks

- Geopolitical & Financial viability risk
- Continuity of product/service

- Theft of critical financial data by vendors/third parties, financial frauds
- Poor credit appraisal support
- Lack of compliance to regulatory requirements

Telecom

- Infringement of intellectual property rights
- Regulatory and compliance risk due to changes in international and domestic laws, rules, policies and tax regulations, Telco-specific laws and regulations.
- Reliance on suppliers for sourcing equipment, network devices, and other components, parts and systems has increased the concentration of risk
- Damages to network and billing infrastructure outsourced to vendor.
- Subscription fraud/roaming fraud, dealer fraud and box-splitting.

Oil and Gas

- Geopolitical risk.
- Dependence on contractor for continuity of product/service.
- Lack of compliance to regulatory requirements.
- Loss of reputation due to cyber threats or unavailability of processing systems for transactions.
- Reliance upon third party transportation and processing facilities.