Third-party vendor risk indicators (IT Governance)

Author: Awase Khirni Syed Ph.D. (University of Zurich, Swiss)

Date: July 9, 2025

To transform IT governance from reactive compliance to predictive, autonomous risk management powered by blockchain, AI and real-time threat intelligence, we need to pro-actively identify various risk indicators, implement critical control bots, predictive risk scoring for cloud assets and implement a self-healing control framework. This would help us in creating a real-time dashboard. Furthermore, this could pave way for creating a dynamic risk transfer marketplace.

Table below outlines various Third-party vendor risk indicators identified, this could help us prioritize risk based on financial impact or operational impact or compliance impact. We can use automated vendor risk assessment tools for continuous monitoring or we could build our own notification system. We could conduct automated regular audits for financial, security and compliance. A key takeaway from this would be to incorporate risk clauses in contracts to assess penalties for breaches and for various exit strategies.

	Financial Risk Indicators	• For assessing vendor's financial health and stability • Impact – Financial instability can lead to sudden vendor collapse, contract breaches, or inability to deliver services
i.	Declining revenue or profit margins	Indicates potential insolvency risk
ii.	High debt-to-Equity Ratio	Over-leveraged, may struggle with obligations
iii.	Late Payments to Suppliers or creditors	Cash flow patterns
iv.	Credit Rating Downgrades	Reduced ability to secure financing
v.	History of Bankruptcy or restructuring	High likelihood of future failure.
vi.	Unstable or Unpredictable Cash Flow	May impact service continuity
vii.	Excessive Reliance on a few customers	Revenue concentration risk
viii.	Unfavorable audit findings	Financial mismanagement signs
	Operational Risk Indicators	• To assess internal processes and efficiency • Operational weaknesses lead to delays, errors and service disruptions
i.	Frequent leadership or management changes	Strategic inconsistency

ii.	High employee turnover rates	Poor culture or instability
iii.	Outdated technology and systems	Inefficiency and security risks
iv.	Lack of automation and digital maturity	Manual processes increase errors
v.	Overdependence on key personnel	Bus factor risk
vi.	Poor disaster recovery and business continuity plans	Long downtimes
vii.	Inadequate capacity scaling	Struggles during demand spikes
viii.	Frequent operational downtimes	Unreliable service delivery
	Compliance and Legal Risks	• To assess regulatory and legal exposure • To assess the impact of legal penalties, contract terminations and reputational damage
i.	Regulatory fines or Sanctions	Non-compliance history
ii.	Pending litigations or lawsuits	Legal liabilities
iii.	Failure to meet industry standards (ISO,SOC, GDPR, HIPPA)	Compliance gaps
iv.	Expired or Missing Licenses/Certifications	Operating illegally
v.	History of Data Privacy Violations	GDPR, CCPA breaches
vi.	Non-adherence to Contractual Obligations	Frequent breaches
vii.	Use of forced or child labour (ESG Risk)	Reputational and legal risks
viii.	Violations of Export Controls or Sanctions	Geopolitical risks
	Cybersecurity and Data Risks	• To assess IT security posture • To assess the impact of data leaks, ransomware attacks, regulatory fines and loss of trust
i.	Past data breaches or cyber attacks	Vulnerable infrastructure
ii.	Weak encryption for data at Rest/Transit	Exposure risk
iii.	No Multi-Factor Authentication (MFA)	-weak access controls
iv.	Unpatched software and Known vulnerabilities	Exploitable flaws
v.	Inadequate incident response plan	Slow breach containment
vi.	Excessive user privileges (no least privilege)	Insider threat risk
vii.	No regular penetration testing	Undetected security gaps

viii.	Shadow IT usage/ unauthorized tools usage	Uncontrolled risks
	Reputational Risk	• To access public perception and trust • To assess loss of customer trust, brand devaluation, and partner attrition
i.	Negative media coverage or scandals	Brand damage
ii.	Poor customer reviews and complaints	Service quality issues
iii.	Association with controversial entities	Guilt by association
iv.	Ethical violations (Fraud, Corruption, Discrimination)	ESG risks
v.	History of Misleading claims or Fraud	Trust erosion
vi.	Frequent Executive Misconduct cases	Leadership integrity issues
	Geographic and Geopolitical Risks	• To assess location-based risks • To assess supply chain disruptions, increased costs and operational halts •
i.	Operations in High-Risk/Embargoes Countries	Sanctions exposure
ii.	Exposure to Trade Wars/Tariffs	Cost fluctuations
iii.	Political Instability (Civil unrest, Wars)	Disruptions
iv.	Currency Exchange Volatility	Financial unpredictability
v.	Poor Local Infrastructure, Internet Service Infrastructure, PowerGrid	Service delays
vi.	Strict Data Localization laws	Compliance complexity
	Supply chain and Dependency Risk	• To assess vendors own supply chain • To assess/estimate production delays, cost overruns and contractual failures
i.	Single-source dependencies	No backup suppliers
ii.	Long lead times for deliveries	Bottlenecks
iii.	History of missed deadlines	Unreliability
iv.	Overuse of subcontractors – 4th and 5th parties	Lack of visibility
v.	Poor inventory management	Stockouts or overstocking
vi.	Dependence on rare/ ethical materials	Sourcing risks
	Performance and Service Risks	• To assess quality and reliability

		• To assess/estimate business disruptions, lost productivity and customer dis-satisfaction
i.	Frequent SLA violations	Missed KPIs
ii.	Low system uptime	Frequent outages
iii.	Slow customer support response times	Poor issue resolution
iv.	Lack of transparent reporting	Hidden problems
v.	Resistance to audits or assessments	Non-cooperation
vi.	Inconsistent service quality	Unpredictable outputs
	Strategic Risks	• To assess long-term alignment • To assess viability, vendor resilience, fails to scale or exists the market
I.	Misalignment with your business needs or goals	Conflicting priorities
II.	Vendors overdependence on your business	High attrition risk
III.	Lack of innovation or R&D Investment	Future obsolescence
IV.	No clear succession planning	Leadership vaccum risk
	Contractual and Relationship Risks	• To assess governance efficiency and effectiveness and partnership • To assess difficult vendor management, disputes and costly exits
I.	Unfavorable contract terms such as auto-renewals, exit penalties	Local in risk
II.	Poor communication and responsiveness	Collaboration issues
III.	History of Disputes with other clients	Conflict patterns
IV.	No clear escalation paths for issues	Unresolved problems