Questions to Consider when Choosing a Third-Party Risk Management Tool

**Note:* *Third-parties include vendor or suppliers.*

Consider the following questions when choosing a technological tool to automate the third-party risk management process.

- Is the tool a SaaS (Cloud-based), internally hosted or a traditional web-based solution?
- Has the tool received an independent attestation? For example, ISO certifications such as 9001, 27001, PCI DSS, Fedramp certified, SOC reports or any other attestations?
- Is the tool a Governance, Risk and Compliance (GRC) tool?
- Does the tool support the third-party risk management (TPRM) process? For example, does the tool identify, assess, analyze, mitigate and monitor inherent and residual risks?
- When identifying inherent risk, does it contain a data classification scheme (i.e. public, non-public, confidential, highly confidential, and PII/PHI)?
- What type of risk assessments does the tool perform? For example, does the tool perform reputational, financial, information security, business continuity, and disaster recovery?
- For reputational risk assessments, do news feeds come through RSS feeds? Do the reputational risk assessments provide a risk score based on a risk tier system (i.e. Tier 1, 2, 3 and 4)?
- For financial risk assessments, is it based on ratio analysis and do the results provide a quantitative risk score?
- For information security risk assessments, what are the control areas that are covered (i.e. Access Control, Network Management, Information Security Compliance)
- Does the tool accommodate business continuity and disaster recovery assessments?
- Does the tool allow procurement or vendor relationship managers to upload contracts and analyze contract terms such as right-to-audit, indemnification?
- What are the data analytics capabilities of the tool? Can the tool capture and track identified inherent and residual risks?

- What are the reporting capabilities of the tool?

- Does the tool enable vendor relationship managers to conduct key performance indicators (KPIs)?

- Does the tool allow a risk-based approach to performing the third-party risk management process?