TPRM Budget Preparation
Checklist

Considerations to assist in preparing for your annual third-party risk management (TPRM) budget planning and discussions.

- [ ] Inventory your third parties, categorizing each by inherent risk to the functioning of your organization.
- [ ] Determine your organization's risk appetite, accounting for your risk capacity and tolerance.
- [ ] Determine the level of effort (LoE) required to manage each third party's risk. Identify what can be automated and what requires human handling and review.
- [ ] Based on the anticipated annual human activity, the cost of TPRM tooling, and solutions to manage risk, calculate how many third-party risk analysts are needed on your team.
- [ ] Plan for staff training:
  - [ ] TPRM tools
  - [ ] Risk assessments
  - [ ] Risk assessment evaluation and treatment processes
- [ ] Project the costs for the estimated third-party incidents you are likely to respond to.
- [ ] Estimate the cost of compensating controls for unresolved third-party risk.
- [ ] Determine the appropriate sized cyber insurance policy, based on the residual third-party risk and estimated third-party incidents you will incur.
- [ ] Prepare a strategy for scaling your team based on corporate growth objectives and anticipated third-party expansion.
- [ ] Factor in compliance and regulatory considerations, including the cost of any required compliance based audits and certifications.
- [ ] Calculate, in dollars and percentages, your TPRM budget according to your third parties, potential losses, and risk appetite.

- [ ] ***Avoid:*** basing your budget based on industry spending stats. Tailor your budget according to your organization's needs.
- [ ] ***Avoid:*** thinking more money equates to better protection. Zero risk is impossible; your objective is to reduce your risk, to bring your risk down to acceptable levels.

Pinpoint, measure, and prioritize your third-party cyber risks so you can plan appropriately and sleep soundly.