**A TPRM Policy Template**

*Below is a template of a Third-Party Risk Management Policy. This includes a ready-to-use template to easily implement a TPRM policy into your business.*

*Follow the below steps to have a functioning TPRM Policy ready to go*

1. *Read through the document & fill in the company information in red*
2. *Add your company logo to the letter head & add your signature to the document*
3. *For support with your TPRM policy or risk management, reach out to our team of experts by emailing* *info@brooklynsolutions.ai*

**Third-Party Risk Management Policy**

**1. Introduction**

[Company Name] recognises the importance of effectively managing risks associated with third-party relationships to safeguard the interests of our customers, protect sensitive information, maintain regulatory compliance, and ensure the resilience of our operations. This Third-Party Risk Management Policy outlines the principles, processes, and responsibilities for managing third-party risks across [Company Name].

**2. Scope**

This policy applies to all third-party relationships, including vendors, suppliers, service providers, contractors, and outsourcing arrangements, that have a material impact on the operations, reputation, or financial condition of [Company Name]. It encompasses the entire lifecycle of third-party relationships, from initial due diligence and vendor selection to ongoing monitoring, contract management, and termination.

**3. Governance and Oversight**

* The Board of Directors is ultimately responsible for overseeing third-party risk management and ensuring compliance with this policy.
* The Risk Management Committee provides oversight and guidance on third-party risk management practices, policies, and procedures.
* The Chief Risk Officer (CRO) is responsible for overseeing the implementation of this policy and ensuring that adequate controls and processes are in place to manage third-party risks effectively.

**4. Risk Management Framework**

[Company Name] employs a risk-based approach to third-party risk management guided by the following principles:

* Risk Identification: Identify and assess risks associated with third-party relationships, including operational, compliance, reputational, cybersecurity, and financial risks.
* Due Diligence: Conduct thorough due diligence on potential third-party vendors to evaluate their capabilities, reliability, financial stability, regulatory compliance, and risk management practices.
* Risk Assessment: Assess the inherent risk and potential impact of third-party relationships based on factors such as the nature of services provided, criticality to business operations, geographic location, and regulatory requirements.
* Risk Mitigation: Implement appropriate risk mitigation measures to address identified risks, including contractual provisions, service level agreements (SLAs), risk-sharing arrangements, and contingency plans.
* Ongoing Monitoring: Continuously monitor third-party relationships throughout the duration of the contract to ensure compliance with regulatory requirements, contractual obligations, and risk management standards.
* Reporting and Escalation: Establish reporting mechanisms to provide regular updates to senior management and the Board of Directors on third-party risk exposures, issues, and mitigation efforts. Escalate significant risks and issues to the appropriate governance bodies for timely resolution.
* Continuity Planning: Develop contingency plans and exit strategies to manage the risks associated with terminating or transitioning third-party relationships, ensuring continuity of critical services and minimising disruption to business operations.

**5. Roles and Responsibilities**

* The Chief Procurement Officer (CPO) is responsible for overseeing the procurement process, vendor selection, and contract negotiations in compliance with this policy.
* The Vendor Management Office (VMO) is responsible for maintaining a centralised inventory of third-party relationships, conducting due diligence, risk assessments, and monitoring activities, and ensuring compliance with regulatory requirements and internal policies.
* Business Units and Departments are responsible for identifying their third-party relationships, assessing their risk exposure, and collaborating with the VMO to manage third-party risks effectively.
* Internal Audit and Compliance functions are responsible for independently assessing the effectiveness of third-party risk management practices and providing assurance to senior management and the Board of Directors.

**6. Compliance and Enforcement**

Non-compliance with this policy may result in disciplinary action, including termination of contracts, removal from approved vendor lists, and referral to regulatory authorities for further investigation. All employees are required to adhere to this policy and report any violations or concerns to their supervisor or the Compliance Department.

**7. Policy Review and Updates**

This policy shall be reviewed annually or as needed to ensure alignment with regulatory requirements, industry best practices, and changes in the business environment. Updates and revisions to this policy shall be approved by the Board of Directors or the Risk Management Committee.

**8. Policy Communication**

This policy shall be communicated to all employees, third-party vendors, and relevant stakeholders through appropriate channels, such as employee handbooks, training programs, and vendor contracts. Employees and vendors are required to acknowledge their understanding and compliance with this policy upon engagement with [Company Name].

**9. Policy Documentation**

A centralised repository shall be maintained to document all third-party relationships, due diligence findings, risk assessments, contractual agreements, monitoring activities, and audit reports in accordance with record-keeping requirements and data protection regulations.

**10. Policy Adoption**

This Third-Party Risk Management Policy shall be adopted by [Company Name] upon approval by the Board of Directors and communicated to all relevant stakeholders for implementation.

**11. Policy Effective Date**

This policy shall become effective upon approval by the Board of Directors and shall remain in effect until superseded or revised by subsequent updates approved by the Board.

**[Company Name]**
[Date]

[Signature of Board Chair or CEO]