Third-Party Risk Management Program

Builder’s Guide

AskDegree

Dear TPRM Program Builder 👷🏽‍♂️,

Third-Party Risk Management (TPRM) has always been a critical aspect of operational excellence. Most businesses leverage third parties on a daily basis to perform critical aspects of company operations. These third-parties can include online SaaS tools, suppliers, vendors, consultants, and strategic business partners.

The TPRM Program is the mechanism businesses should use to monitor and manage risks exposed to the company by way of third-party relationships.

You may have received the charge to whip your company’s TPRM program into shape, and perhaps you could use some help in navigating this hefty endeavor.

In this quick guide, we will explore the best practices of TPRM, providing you with the knowledge and tools to strengthen your TPRM development strategy.

Sincerely,

AskDegree Launchpad Team

👨🏽‍🚀👨🏽‍🚀👨🏽‍🚀🚀

1. Know Your Regulatory Landscape

AskDegree°

1. Know Your Regulatory Landscape

The first layer of TPRM oversight involves navigating the complex regulatory landscape. Regulations in the fintech industry are constantly evolving, and staying up-to-date with how regulatory risks apply to your unique environment is crucial. This can be challenging, as different jurisdictions, products, and target customers may have unique regulatory obligations. To effectively navigate the regulatory landscape, consider the following practices:

1.1 Building a Regulatory Compliance Framework

Step one, is to develop a robust regulatory compliance framework that outlines your company's obligations and provides clear guidance on compliance management. This framework should include policies and procedures that address specific regulations, risk assessments, compliance training programs, and a process for monitoring and reporting compliance issues.

Knowing your compliance obligations will allow you to understand what risks extend into your third-party relationships. This insight provides the foundation for risk areas you will want to check when performing due diligence.

1.2 Understanding Regulatory Changes

After you have carved out an adequate understanding of your compliance obligations, you must stay informed about regulatory changes. Establishing a mechanism to monitor regulatory movement continuously is paramount to ensuring the TPRM controls remain effective.

Keeping your pulse on the regulatory landscape may involve subscribing to regulatory updates, participating in industry forums and events, following industry subject matter experts on LinkedIn, and engaging with regulatory authorities. By proactively monitoring and analyzing regulatory changes, you can ensure that both your company and your third-party partners remain compliant as well; improving odds that potential penalties or reputational damage is avoided.

1.3 Engaging with Regulatory Authorities

Establish open lines of communication with regulatory authorities. Building relationships with regulators can help you better understand their expectations and requirements. In instances where you may feel apprehensive or simply not know the best route toward direct communication with regulators, seek guidance from experienced compliance consultants who have established relationships with regulatory authorities. They can provide valuable insights and support in your interactions with regulators.

2. Build Full-Cycle TPRM Oversight

2. Build Full-Cycle TPRM Oversight

The second layer involves the development of the actual TPRM Program. Outsourcing operational tasks to third-party vendors will introduce additional compliance risks, and it is crucial to go into these relationships with your eyes wide open as it relates to risks. Conducting regular risk assessments at the top of the relationship, throughout the relationship, and at the close of the relationship will put your company in the best position to mitigate these risks. To enhance your third-party risk management efforts, consider the following practices:

2.1 Vendor Due Diligence

Conduct thorough due diligence on potential third-party vendors before entering into any business relationships. Evaluate their compliance programs, privacy practices, financial stability, security measures, reputation, and general track record. This may involve roping in the procurement, legal, and finance teams to ensure these checks are done before a commitment has been made. Completing this review at the top of the relationship ensures that you partner with vendors who align with your compliance standards and have a strong commitment to regulatory compliance.

2.2 Contractual Agreements

Work with your legal department to establish clear contractual agreements with third-party vendors that outline their compliance obligations, data protection measures, uptime, and the process for monitoring their performance. Include provisions for audits, incident response, and termination of the relationship in the event of non-compliance. Your legal team should establish baseline provisions to be adopted across the majority of your vendor contracts, this helps to establish a consistent level of contractual protection for the company. Regularly review and update these agreements to reflect changing regulatory requirements and industry standards.

2.3 Ongoing Monitoring and Audit

Implement a robust monitoring and auditing program to assess the ongoing compliance of your third-party vendors. Regularly review their performance, conduct audits, and monitor their adherence to contractual agreements. This proactive approach helps identify and mitigate any potential compliance risks before they escalate.

2.4 Continuity Planning

Although the onboarding diligence should help you to identify possible continuity risks; unforeseen events can happen that could cause a temporary or permanent disruption to your vendor's ability to continue services. The development of a comprehensive continuity plan for critical vendors is a best-practice approach. Assessing the impact of service interruption, identifying alternative vendors or contingency plans, and implementing measures to ensure business continuity are all a part of this step. Regularly test and update your continuity plan to address emerging risks and changing business needs.

3. Leverage Consultant Expertise

AskDegree°

3. Leverage Consultant Expertise

Navigating the complex landscape of TPRM can be challenging, especially for companies with limited resources or expertise. By leveraging the expertise of consultants, you can often accelerate the development time frame for your TPRM program and quickly enhance your compliance management efforts. Consider the following practices when engaging with compliance consultants:

3.1 Selecting Experienced Consultants

Choose consultants with extensive experience and a deep understanding of integrating third-party risk management processes and workflows. Look for consultants who have worked with companies similar to yours and have a proven track record of delivering effective compliance solutions.

3.2 Tailored Compliance Solutions

Work with consultants who can tailor their services to meet your specific compliance needs. They should understand your business model, operational processes, and unique compliance challenges. This ensures that their recommendations and solutions are aligned with your company's objectives, capabilities, and culture.

3.3 Continuous Support and Guidance

Engage consultants who provide ongoing support and guidance beyond the initial engagement. Compliance requirements evolve over time, and having a trusted advisor who can help you navigate these changes is invaluable. Look for consultants who offer regular check-ins, updates on regulatory developments, and access to their expertise when needed.

4. Embrace an Iterative Approach

AskDegree

4. Embrace an Iterative Approach

The final layer to the successful development of a TPRM program is to embrace the spirit of iteration. Third-party risk management is not a one-time task but an ongoing process that requires continuous improvement and adaptation. Embrace an iterative approach to TPRM by regularly assessing and enhancing your practices. Consider the following guidance to foster an iterative compliance management mindset:

4.1 Continuous Pursuit of Optimization

Conduct regular analysis to determine which processes could be automated, condensed, and ultimately streamlined. This could include the introduction of technological enhancement and the deployment of third-party contract management platforms.

4.2 Continuous Training and Education

Stay updated on industry best practices and regulatory changes by investing in continuous training and education. Encourage employees to participate in relevant webinars, workshops, and conferences. This helps foster a culture of continuous learning and ensures that your TPRM practices remain up-to-date with industry best practices.

4.3 Continuous Monitoring and Evaluation

Implement a robust monitoring and evaluation system to track the effectiveness of your compliance management efforts. This monitoring and testing layer should reside outside of the TPRM function, allowing for the independence of reviews. TPRM staff should then regularly review key performance indicators, audit findings, and incident reports to identify areas for improvement and optimization.

Conclusion

Effective third-party risk management is crucial for protecting customer and investor interests, and ensuring long-term success. By maintaining a clear picture of your company's compliance footprint and obligations, management of third-party influence toward your organization's risk posture is greatly improved. Remember, TPRM is not a one-time task but an ongoing commitment to ethical and responsible business practices. Stay proactive, stay informed, and continuously adapt your efforts to remain competitive and compliant.

Visit AskDegree for the latest risk management and compliance trends impacting the fintech industry.