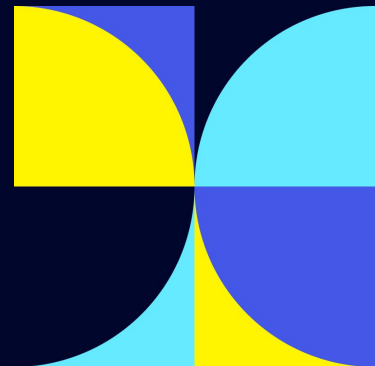
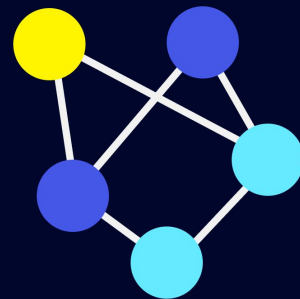


SEPTEMBER 2024

Effective TPRM: Why good intentions aren't enough




Why is Third Party Risk Management (TPRM) important?

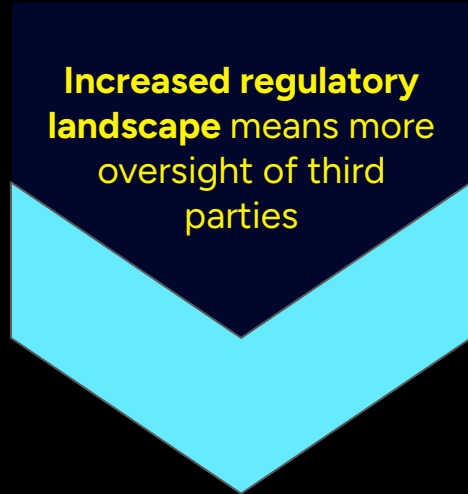
TPRM impacts every business



Companies
approaching **100%**
third party owned tech
stack



**Most security
breaches** happen via
third party vendors



**Increased regulatory
landscape** means more
oversight of third
parties



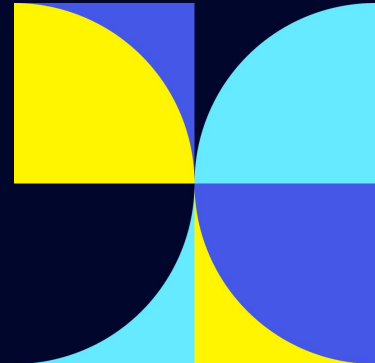
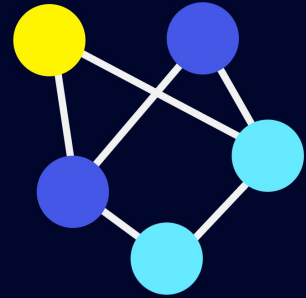
TPRM Conundrum

Operational issues lead to painful tradeoffs

Most TPRM programs focus their limited resources on the tip of the iceberg.

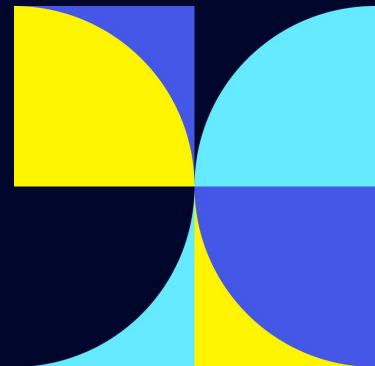
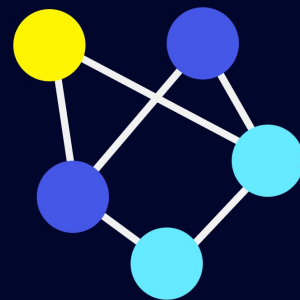


4 Counterintuitive practices that undermine your third-party risk strategy:



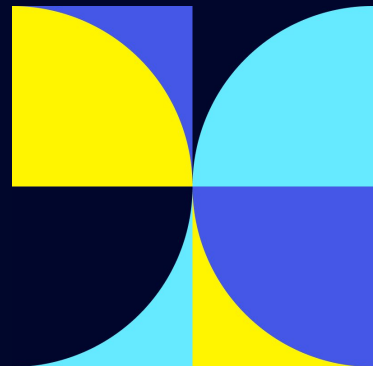
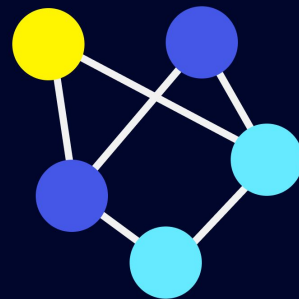
1. Choosing a slow review over no review

Slow assessments delay critical decision-making, leaving businesses exposed to unmitigated risks while waiting for approvals.



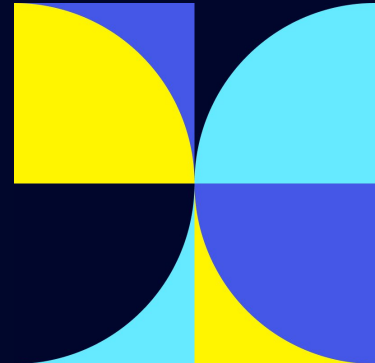
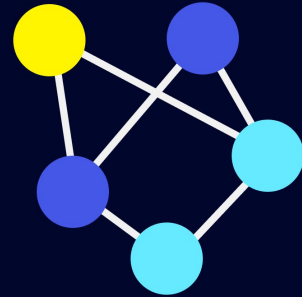
2. Assessing a vendor solely after signing a contract with them

Post-contract evaluations miss key risk indicators: Waiting until after a contract is signed limits the ability to address risks early, leading to inefficiencies and greater potential for unexpected issues.



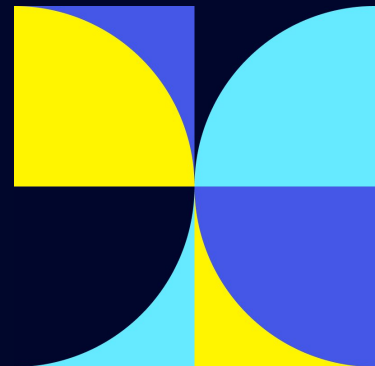
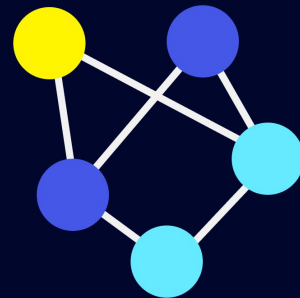
3. Basing your vendor evaluation thresholds on dollar amounts or other criteria

Basing risk thresholds on contract value overlooks true risk:
Relying on financial or arbitrary thresholds fails to account for non-financial risks like security vulnerabilities, regulatory non-compliance, or reputational damage.

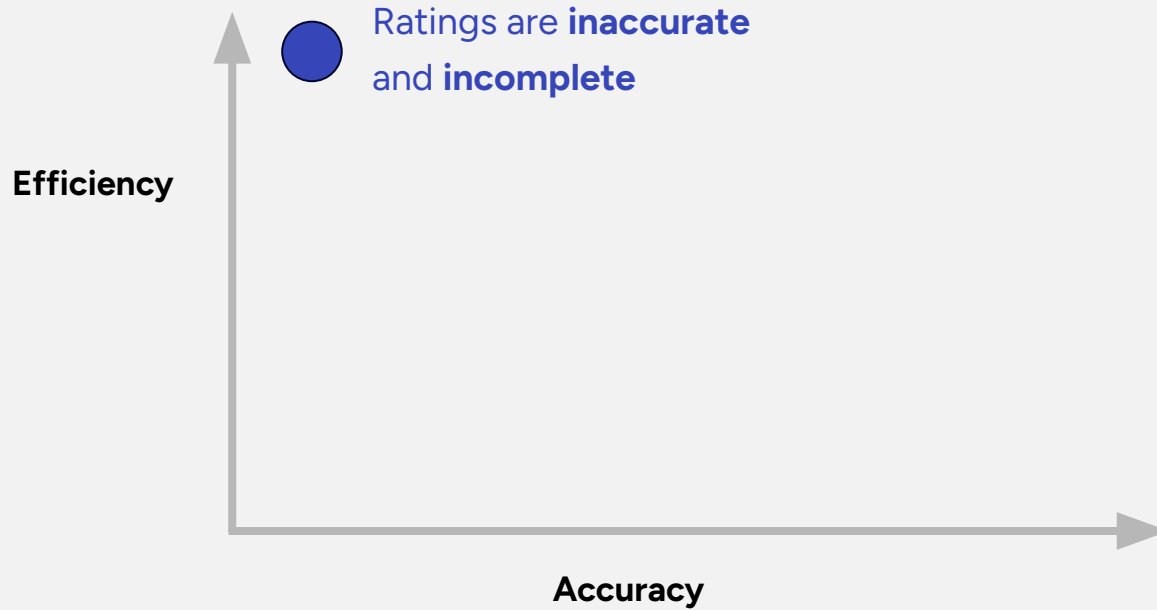


4. Relying on questionnaires and ratings

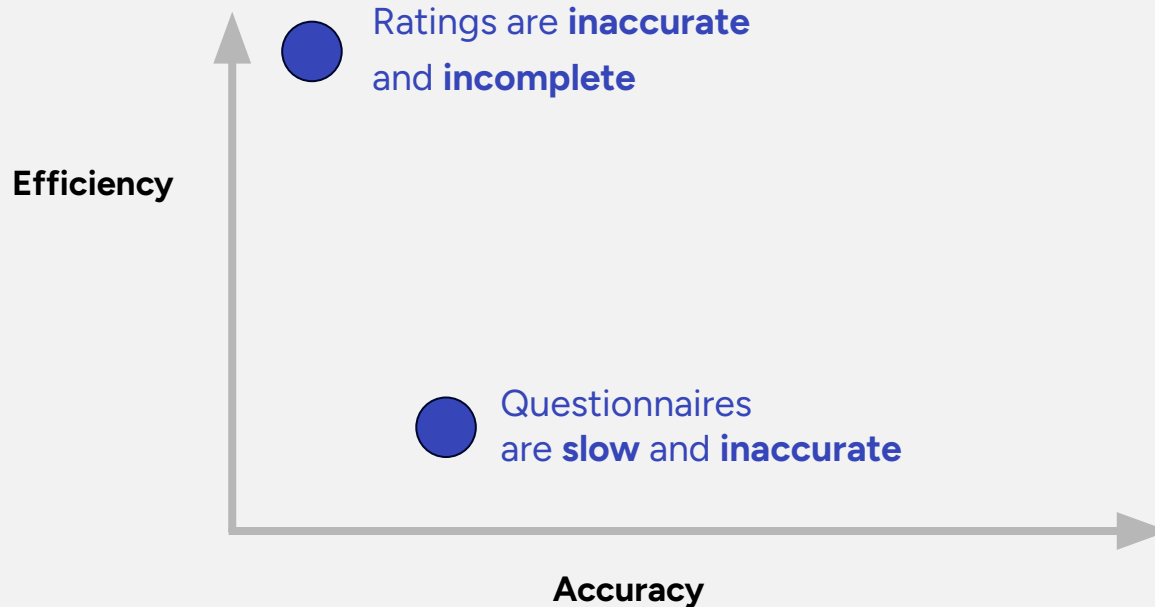
Over-reliance on questionnaires leads to shallow insights: Questionnaires alone often generate superficial data, adding busy work without a comprehensive understanding of a vendor's true risk profile.



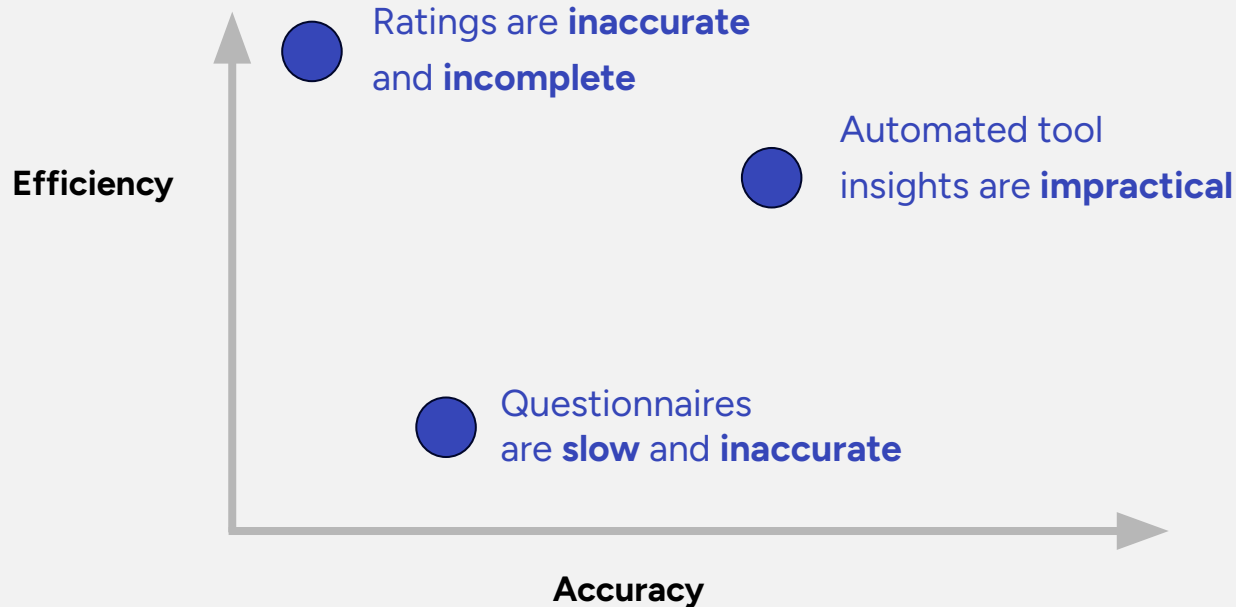
Existing approaches come with significant tradeoffs



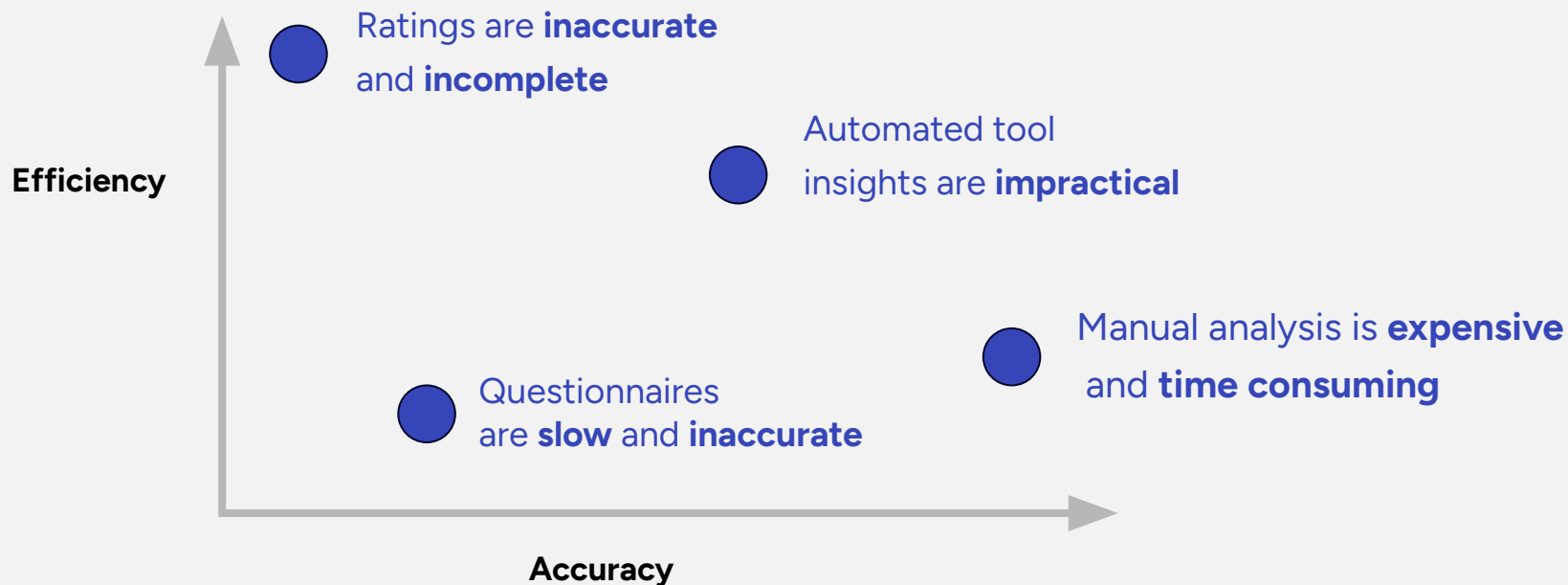
Existing approaches come with significant tradeoffs






Existing approaches come with significant tradeoffs



Existing approaches come with significant tradeoffs



Unintended Consequences of Poor TPRM

-  **Erosion of Business Relationships:** Inadequate risk management can weaken trust with partners, leading to breakdowns in communication and collaboration.
-  **Increased Vulnerability:** Poor TPRM can open up organizations to additional risks, including security breaches and operational inefficiencies, due to neglected third-party relationships.
-  **Impact on Reputation and Compliance:** Failed partnerships can damage a company's reputation and expose it to regulatory scrutiny, resulting in penalties or loss of business.



TPRM Program Misalignment

TPRM is at odds with the needs of the business

Slow and unreliable processes, and opaque and inconsistent results undermine the culture of security and risk management and lead to frustration and ultimately risk apathy among stakeholders.



Critical Role of TPRM in the Modern Business Environment



Enhanced Security Posture: TPRM helps organizations identify and mitigate risks associated with third parties, strengthening their overall security posture.



Improved Compliance and Regulatory Adherence: TPRM ensure compliance with industry regulations and data privacy standards, minimizing the risk of fines and penalties.



Reduced Business Disruptions: Effective TPRM practices minimize the impact of third-party security breaches and disruptions to business operations.



Enhance Reputation and Trust: Demonstrating strong TPRM practices builds trust with customers, partners, and investors, enhancing the organization's reputation.



Effective third party risk management is more than a safeguard--it's the ability to rapidly innovate while eliminating risk.




In short, it's a competitive advantage."



Alexander Hughes
Information Technology and Compliance Executive



Sustaining Partnerships Through Effective TPRM

-  **Building Trust:** Implementing proactive risk management practices fosters transparency and trust between organizations and third-party vendors.
-  **Continuous Monitoring:** Highlight the need for ongoing evaluation and monitoring of third-party relationships to ensure long-term sustainability.
-  **Collaborative Risk Mitigation:** Emphasize the importance of working with third-party partners to mitigate risks collaboratively, aligning business goals and risk management strategies.

Balancing Risk and Business Initiatives

Navigating the delicate balance between risk and business growth is crucial for companies aiming to achieve success. It's about finding the right path that allows companies to embrace innovation and expand without jeopardizing their stability.



Collaborative Risk Mitigation



Collaboration is crucial to mitigate risk effectively.



Third-party partnerships allow organizations to share knowledge, resources, and expertise, leading to better risk management practices.



These partnerships enhance learning, achieve business goals, and drive effective risk mitigation strategies.



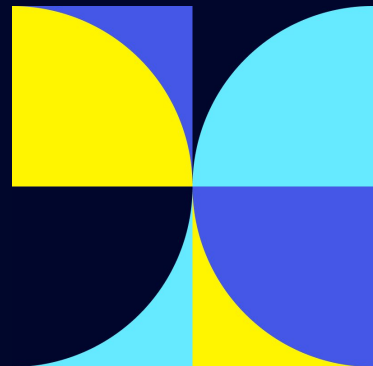
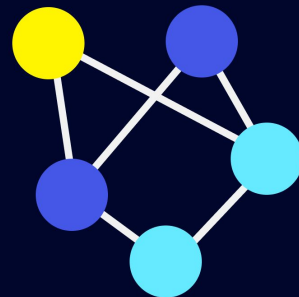
The Future of TPRM: Adapting to Emerging Risks



Adapting to Emerging Risks: TPRM must adapt to the evolving threat landscape. It's essential to incorporate new technologies and best practices into your security strategy.



Proactive TPRM: TPRM is no longer just reactive. It is critical to proactively identify and mitigate risks before they can cause harm.



Reshaping the TPRM Landscape



AI-Powered Risk Assessment: AI algorithms analyze vast amounts of data to identify emerging threats and vulnerabilities, providing proactive risk assessment.

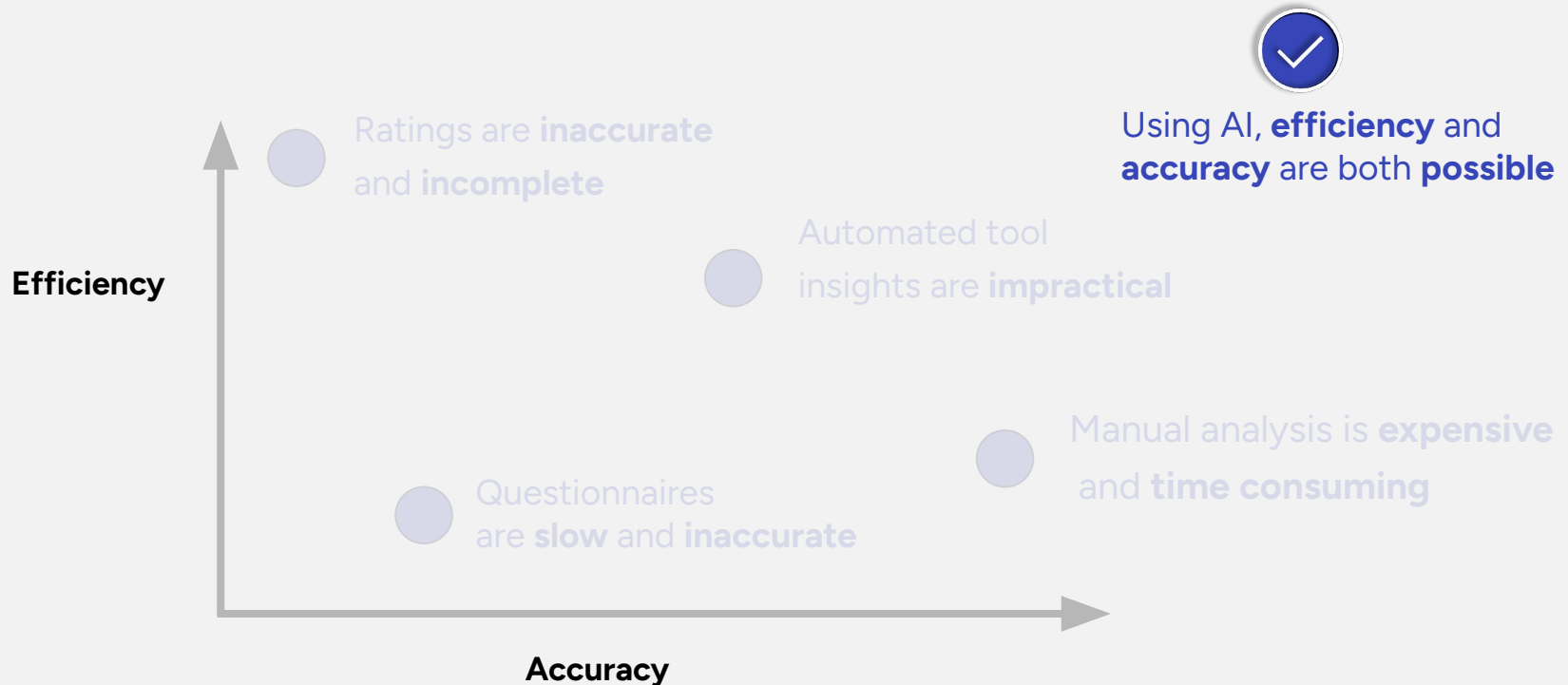


Automated Due Diligence and Monitoring: Automation streamlines due diligence processes, enabling continuous monitoring of third-party risk profiles and compliance.



Data Analytics for Proactive Insights: Data analytics provide valuable insights into risk trends, enabling organizations to anticipate and mitigate potential threats.

AI-powered automation unlocks TPRM value through operational excellence



Key Takeaways: The Importance of TPRM



Enhanced Trust: By proactively managing risks, organizations can build stronger relationships with their third parties, based on mutual trust and understanding.



Increased Resilience: TPRM helps to identify and address potential risks, minimizing disruption and ensuring business continuity, even in challenging situations.



Sustainable Partnerships: By working collaboratively with third parties manage risks, organizations can foster long-term partnerships that benefit both sides.

CALL TO ACTION



Conduct Risk Assessments: Really assess service associated with your third parties, taking into account factors such as industry, location, and the nature of the relationship



Establish Clear Contacts: Define clear expectations and responsibilities and contract with third parties, including mitigation measures, and performance standards.



Implement Monitoring and Reporting: Continuously monitor third-party performance and risk profiles, and implement appropriate reporting mechanisms to ensure transparency and accountability.



Paul Valente

CEO & Co-Founder of VISO TRUST

Paul is a former CISO and built successful security teams and programs at ASAPP, LendingClub, and Restoration Hardware

Connect with us

Email

paul@visotrust.com

LinkedIn

<https://www.linkedin.com/in/pauldvalente/>

Learn more about VISO TRUST

www.visotrust.com