TrustWorks 360

Respecting Data, Improving Trust.

Third-Party Risk Management (TPRM):

Shoring Up Your Defences in a Connected World

Imagine your organisation as a well-fortified castle. You've invested in robust security measures to protect your data, the crown jewels of your business. But what about the drawbridge you use to interact with the outside world? Third-party vendors and partners – those who provide essential services – act as these access points. If their defences are weak, or even worse, you invite a Trojan horse in, your entire castle becomes vulnerable.

Third-Party Risk: A Hidden Threat

In today's digital age, organisations rely heavily on third-party vendors for various services, from cloud storage, marketing automation and even outsourced business processes. While these partnerships offer undeniable advantages, they also introduce risk. Smaller or less security or privacy conscious vendors are an easier target for cybercriminals seeking a backdoor into your organisations or systems. A data breach at a vendor can have a domino effect, compromising your sensitive information and potentially impacting your customers.

TPRM: Old process for new risks

Existing TPRM process vary greatly between organisations. Even very large organisations are still using spreadsheet assessments developed by IT or the cyber team to assess the risks of an organisation to be used to provide a product or service. Often these assessments have significant issues including:

- **One size fits all**: assessments are not focussed on the level of risk introduced by a third party and therefore not prioritising mitigation effort: i.e. putting most effort into third parties that introduce the most risk.
- **Stand-alone, once off**: risk assessment that are not integrated into any other risk or monitoring systems and therefore done as a once off exercise that doesn't track changes to the risk profile from changes by the third party or the use of that third party within your organisation.
- **Manual, Decentralised:** someone sending a spreadsheet in an email, getting completed by the vendor and returned by email. No central repository or dashboard to ensure all business areas are complaint and all third parties, inlcuding AI providers are assessed at approrirate time intervals.
- **Narrow**: while these risk assessments are typically (and rightly) focussed on cyber security and IT related risks that is not the only sources of risk. Assessing other aspects of risk such as vendor business stability, ethics and their ESG practices can provide a much clearer picture of the overall risk associated with partnering with the third party.

Third-Party Risk Management: Building a Stronger Bridge

Third-party risk management (TPRM) is the essential strategy for mitigating the risks associated with vendors and ensuring the secure handling of your data. A well-defined TPRM program empowers you to:

- **Proactively Identify Risk:** Systematically and regularly assess potential security, privacy and other risks each thiurd party vendor poses. Consider factors like the criticality of their services, the level of integration with your systems, and the type of data they access or hold on your behalf.
- **Collaborative Security and Privacy Measures:** Develop and implement security and privacy protocols in collaboration with your vendors to safeguard your data. These controls may include encryption standards, access control mechanisms, data retention or minimisation and clear incident response procedures.
- **Continuous Monitoring:** Don't set it and forget it. Regularly monitor vendor security and privacy practices to ensure they remain effective. This can involve automated, periodic security assessments, reviewing vendor security reports, and leveraging automated tools that provide real-time insights into vendor risk posture.
- **Full risk picture: consider other risk domains:** The risks introduced by third parties and vendors don't stop with IT or cyber security. Risks to an organisation can come from a range of other areas such as ethics and ESG, and these should be considered when assessing the risk of introducing third party into an organisation.

Taking Action: Building a Secure Third-Party Ecosystem

Here are some critical steps you can take to strengthen your TPRM program:

- **Standardise Vendor Assessments:** Develop an effective (for you and your vendor), standardised approach to evaluating vendor risk in a suite of re-usable templates suited to the type of vendor and level of risk. This could involve targeted questionnaires, security audits, reviewing applicable certifications or leveraging automated monitoring and assessment tools.
- **Integrate Risk Assessments with GRC Business Processes:** Don't assess risk in isolation. Integrate risk information with procurement and contracting processes to ensure you partner with security-conscious vendors.

- **Prioritise and Automate Ongoing Monitoring:** Move beyond one-time assessments. Continuously monitor vendor security throughout the lifecycle of your partnership. The frequency and depth of monitoring should be based on the level of risk each vendor presents and should use monitoring services that link directly to your TPRM platform, alerting you to changes in risk for action in real time.

Partnering for a Secure Future

Managing third-party risk is an evolving process that can be greatly improved. By implementing a robust TPRM program using technologies and services to support the program, you can build a far more secure and resilient third-party ecosystem. This protects your business, your data, and fosters trust with your customers and partners.

Ready to Discuss Your Third-Party Risk Management Needs?

We understand the complexities of managing vendor risk in today's ever-evolving threat landscape. Our team of experts can help you develop a comprehensive TPRM strategy that safeguards your data and strengthens your overall security posture. Contact us today to discuss how we can help you build a secure bridge to a connected future.

TRUSTWORKS360 PYT LTD

Email: Contact@trustworks360.com

LinkedIn: Trustworks360 LinkedIn

Website: Trustworks360 Website