Third Party Risk Management (TPRM) in the UK

Third Party Risk Management (TPRM) is the practice of identifying, assessing, and mitigating risks associated with engaging with third-party vendors, suppliers, contractors, or partners. It involves implementing processes and controls to ensure that third parties meet the organisation's standards for security, privacy, compliance, and operational resilience.

When organisations engage with third parties, they introduce potential risks that can impact their operations, reputation, and compliance obligations. These risks can arise from various factors, including:

Data security and privacy:

third parties may have access to sensitive data or systems, making it crucial to assess their security controls, data handling practices, and adherence to privacy regulations

Financial stability:

the financial health and stability of third parties can impact their ability to deliver services or products effectively. Assessing their financial standing helps mitigate the risk of service disruptions or contract terminations

Business continuity:

third parties may provide critical services or products, and their failure to deliver can disrupt operations. Assessing their business continuity plans and resilience measures is important to mitigate such risks

Regulatory compliance:

organisations are responsible for ensuring that their third parties comply with applicable laws, regulations, and industry standards to avoid legal and regulatory penalties

Reputational risk:

the actions or misconduct of third parties can reflect badly on organisations that associate with them, so it's important to monitor your third-party relationships

Third Party Risk Management helps organisations identify and address potential vulnerabilities, strengthen their resilience, and safeguard their reputation. It is a critical component of a robust GRC programme, ensuring that third-party relationships align with an organisation's risk platform and compliance requirements.

The need for TPRM

Engaging with third-party vendors, suppliers, and partners exposes organisations in the UK to various risks that can impact their operations and compliance.

64%

of UK organisations experienced a data breach through a third part in 2020*

82%

of UK organisations believe third-party risks will increase in the next two years**

Inadequate third-party risk management can lead to reputational damage, regulatory non-compliance, financial losses, and data breaches.

Benefits of TPRM

- **Mitigates data breach risks:**
  proper TPRM reduces the likelihood of data breaches caused by third parties, protecting sensitive information
- **Ensures regulatory compliance:**
  TPRM helps organisations meet regulatory obligations by ensuring third parties adhere to relevant laws and standards
- **Enhances operational resilience:**
  effective TPRM strengthens an organisation's ability to manage disruptions caused by third-party failures
- **Protects reputational value:**
  robust TPRM safeguards an organisation's reputation by minimising risks associated with third-party misconduct

How do we help?

Our specialists bring with them a number of capabilities, providing organisations like yours with the knowledge and resources needed to manage your third-party suppliers safely and securely. Our specialists help with:

Risk identification:
identify and categorise third parties based on their criticality and potential risk exposure to your organisation

Due diligence:
conduct thorough assessments and due diligence on third parties before engaging with them. This may include evaluating their financials, security practices, regulatory compliance, and references

Contractual controls:
establish contractual terms and agreements that clearly outline the expectations, responsibilities, and compliance requirements for third parties

Ongoing monitoring:
continuously monitor and assess third parties throughout the relationship to ensure ongoing compliance, security, and performance

Incident response planning:
develop incident response plans that outline the steps to be taken in the event of a security breach, compliance violation, or disruption caused by a third party

Take the next steps

Third Party Risk Management is crucial for organisations in the UK to identify, assess, and mitigate risks associated with engaging third parties.

Book a free one-to-one call with one of our GRC (governance, risk, and compliance) specialists to discover how to implement secure TPRM.

Book now

https://calendly.com/security-governance-risk-compliance-and-environment/supplier-assurance-third-party-risk-management-trpm

*Ponemon Institute, "2021 UK Cost of Data Breach Study"
**Deloitte, "Extended Enterprise Risk Management Global Survey 2020"

Contact us

hello@phoenixs.co.uk
01904 562200