# Third-party risk management (TPRM)

## Managing risks in the energy and infrastructure sector

September 2023

pwc

# Third-party risks in energy and infra companies

## Compliance risks

Energy and infrastructure companies are challenged by potential involvement with third parties engaged in non-compliance with regulatory standards. This poses a significant risk in terms of legal repercussions, reputation damage and potential disruptions to operations.

## ESG risks

Energy and infrastructure firms value ESG principles but struggle to apply them to third-party partners. Working with non-compliant entities risks reputation harm, regulatory attention, and stalled sustainability efforts.

## Operational risks

Energy and infrastructure companies rely heavily on third parties for smooth operations. Inadequate due diligence on third-party capabilities, reliability, and performance can lead to operational failures, project delays and unexpected costs.

## Risk related to labour practices

Energy and infrastructure companies must prioritise fair labour practices. Neglecting ethical labour practices in third-party partnerships may lead to legal trouble, reputation damage, and moral concerns.

## Management risks

Energy and infrastructure companies encounter challenges when delegating critical functions to external parties. These challenges encompass potential goal misalignment, insufficient oversight, and suboptimal decision-making. Inadequate management of these aspects can undermine project outcomes and impede the companies' growth trajectory.

## Cyber security/privacy

Energy and Infrastructure companies struggle with cybersecurity when working with third parties. Sharing sensitive data poses risks related to cyberattacks, breaches, and privacy violations, leading to operational disruptions and information compromise.

## Financial risks

Energy and infrastructure firms risk financial instability due to unreliable third-party finances or fraud. Inadequate due diligence can lead to unpaid invoices, project disruptions, and losses, underscoring the importance of careful partnership assessment.

# Importance of third-party risk management

In a complex business landscape, collaborating with third parties offers benefits such as cost efficiency, expertise, and technological advancements. However, these gains must be weighed against emerging risks. Increasing concerns regarding third parties include disruptions in services and breaches. Emerging risks, such as interruptions in services and business failures, directly affect the reputation and operations, and even lead to penalties in some cases. In recent times, instances of third-party risks are rising, with the most prominent concerns being customer service interruptions and breaches of regulations.

Managing third-party risks is crucial for an energy and infrastructure company to ensure operational stability, compliance, and reputation protection. It is crucial for the companies to better assess their readiness and develop a comprehensive strategy to manage third-party risks, safeguard their operations, and maintain a competitive edge in the industry.

## Questions to start with…

### Does your company have a right administrative model to manage third-party risks?

- Clear third-party definition and associated risk visibility
- Mechanism for crisis response and mitigation
- Defined roles and responsibilities for risk management
- Defined outsourcing and third-party strategy with risk appetite

### Does your company have a suitable framework to manage and reduce third-party risks?

- Uniform implementation of TPRM programme across the organisation
- Assessment team with the right expertise and sufficient capacity
- Risk assessment process before contract decisions
- Continuous contract validity tracking

### Does your company have an effective due-diligence processes?

- Data collection and verification methods
- Identifying and evaluating potential risks
- Ensuring adherence to laws and regulations
- Using due diligence in informed decision-making

### Does your company have clearly defined roles and responsibilities?

- Clear job descriptions and understanding of responsibilities
- Well-defined hierarchy and minimal overlap in departments
- Established KPIs aligned with roles
- Effective role communication and interdepartmental collaboration

### Does your company have adequate monitoring and reporting mechanism?

- Monitoring ongoing work
- Regular stakeholder updates
- Real-time issue resolution
- KPI tracking and communication method

## Compliance risks

Third-party non-compliance risks - legal, reputation, operational disruptions, regulatory consequences

## Operational risks

Dependency on third parties: operational failures, delays, unexpected costs, compromised performance

## Management risks

Delegating functions: goal misalignment, oversight gaps, suboptimal decisions, project setbacks, growth impediment

## Financial risks

Unreliable third-party finances: fraud, unpaid invoices, project disruptions, financial losses, partnership assessment

## ESG risks

ESG non-compliance risks: reputation, regulatory, sustainability setbacks

## Risks related to labour practices

Risks involving legal risks, reputation harm, ethical dilemmas, and partnership vulnerabilities

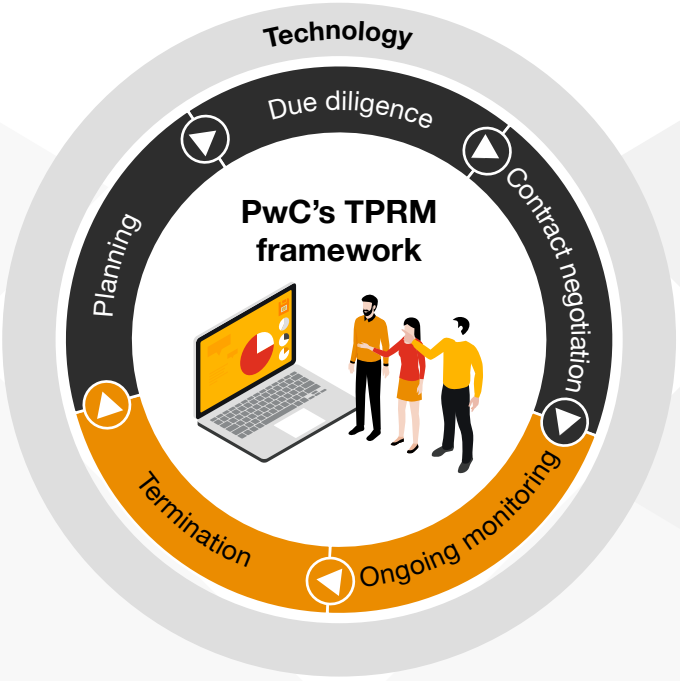
## Cyber security/ privacy

Cybersecurity challenges with third parties: data breaches, operational disruptions, privacy violations

## Cornerstone principles of an effective TPRM programme

**A robust TPRM framework is focused on understanding and managing risks associated with third parties with which the company does business and/or shares data, to strengthen the organisation's position and build more effective partnerships that protect the brand and business.**

| Third parties |
| --- |
| Vendors |
| Suppliers |
| Joint ventures |
| Business channels |
| Marketing partners |
| Affiliates |
| Subsidiaries |
| Regulated entities |




| Risk considerations |
| --- |
| Reputational |
| Operational |
| Credit/financial |
| Business continuity and resiliency |
| Regulatory/compliance |
| Concentration |
| Strategic risks (environmental, cyber, and physical security) |
| Info security and privacy |
| Compliance |

## Suggested steps for third-party risk management (TPRM)

**01** Outsourcing risks to be assessed around compliance, operations, management, finance, ESG, risks related to labour practices, and cyber security/privacy risks.

**02** Defined roles and responsibilities of senior management and the board.

**03** Ensure utmost confidentiality, prioritise data security by granting third-party access to sensitive information strictly on a 'need-to-know' basis, in adherence with industry regulations.

**04** Verify that service providers undertake routine testing of their continuity and recovery strategies. Furthermore, they should partake in occasional joint testing and recovery drills with their service providers.

**05** Elevate operational efficiency through strategic outsourcing of non-core functions, encompassing IT, HR, facilities management, logistics, and marketing, but refrain from outsourcing core management functions, including internal audit, compliance and decision-making functions.

**06** Establish management framework to oversee and regulate outsourcing operations. Regular audits by internal or external auditors should evaluate the effectiveness of risk management practices in overseeing outsourcing, including the company's adherence to its risk management structure and relevant guidelines. Annual evaluations of the financial and operational status of the service providers must be conducted to determine their capability to uphold outsourcing commitments.

**07** Formulate a comprehensive outsourcing policy, sanctioned by the board, encompassing criteria for selecting activities to outsource, choosing service providers/vendors and establishing parameters to define substantial outsourcing engagements.

**08** Conduct comprehensive due diligence of service provider/vendor capabilities, including:

1. assessing past experience and implementation proficiency.
2. scrutinising security, internal controls, audit coverage, reporting, monitoring protocols, and business continuity strategies.
3. verifying the service provider/vendor's due diligence on their staff.
4. ensuring continuous monitoring and assessment through contractual provisions.
5. securing rights for audits, access to audit/review reports, and findings concerning the service provider/vendor.

# How to optimise your existing TPRM programme?

The TPRM programme is an ongoing and continuous process driven by constant programme uplifts, process optimisations and innovations.

## Strategy and oversight

- **Applicable laws and standards**
- **Policy and SoPs**
- **Set and maintain global standards**
- **Central governance, oversight and guidance**

**Data sources:**
Public databases, information provided by third parties, internal transactional data from CRMs and ERPs

### Exiting/ new third parties

- Third-party identification
- Third-party evaluation
- Third-party selection
- Third-party on-boarding
- Third-party termination

### Third-party prioritisation

**Materiality**
- Spend
- Revenue
- Strategic importance
- Single source

**Third-party profile**
- Inherent risk
- Services/goods categorisation
- Terms of trade

**Geographical location**
- Geopolitical stability
- Corruption index
- Availability

**Third-party risk coverage**
- Review method
- Frequency of review
- Reporting

### Third-party risks addressed

1. Financial risks
2. Operational risks
3. Management risks
4. AML/KYC and other compliances
5. Risks related to labour practices
6. ESG risks
7. Cyber and information security

### Risk assessment approach

- Self-assessment (questionnaire)
- Desk research
- On-site inspection
- Off-site inspection
- Hybrid

## Assess, monitor and remediate

**Tool: Third-party risk tracker**

| Modules to customize | Dashboards/ scorecards | Workflows | Audit trail | Risk assessment |
|---|---|---|---|---|

# About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 328,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.



## Contact us

**Puneet Garkhel**
Partner – Risk Consulting
PwC India
+91 98203 20181
puneet.garkhel@pwc.com

**Sunil Mehta**
Partner – Risk Consulting
PwC India
+91 98710 11450
sunil.mehta@pwc.com

**Mitun Bhattacharjee**
Director – Risk Consulting
PwC India
+91 88794 86112
mitun.bhattacharjee@pwc.com

**Omkar Kude**
Director – Risk Consulting
PwC India
+91 90043 90619
omkar.k.kude@pwc.com

pwc.in

Data Classification: DC0 (Public)



HS/September 2023 - M&C 31630