

PwC's integrated third-party risk management (TPRM) tool: Risk Protect

October 2024



TPRM challenges in the current market scenario

Key challenges

PwC's integrated TPRM solution to address key challenges



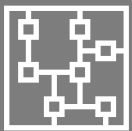
Manual/partially automated approach to third-party onboarding

Automated third-party onboarding and risk assessment tool covering workflow management, third-party due-diligence, contract documentation management and reporting platform



Fragmented risk assessment framework to address various risks faced due to third party

Comprehensive **inventory of third parties** enabling clients to define **criticality** depending on various **risks and mechanism to initiate respective risk assessments** within the application



High upfront investment (cost, resources and time) for implementing a TPRM tool

Lower cost of implementation leveraging start-of-art technology, intuitive onboarding experience and cloud-based deployment model



Inefficiency and lack of agility as third-party management teams operate in silos

Operating a **centre of excellence (CoE)-based managed services model** to assist clients in executing **risk assessment processes, risk classifications and mitigation strategies**



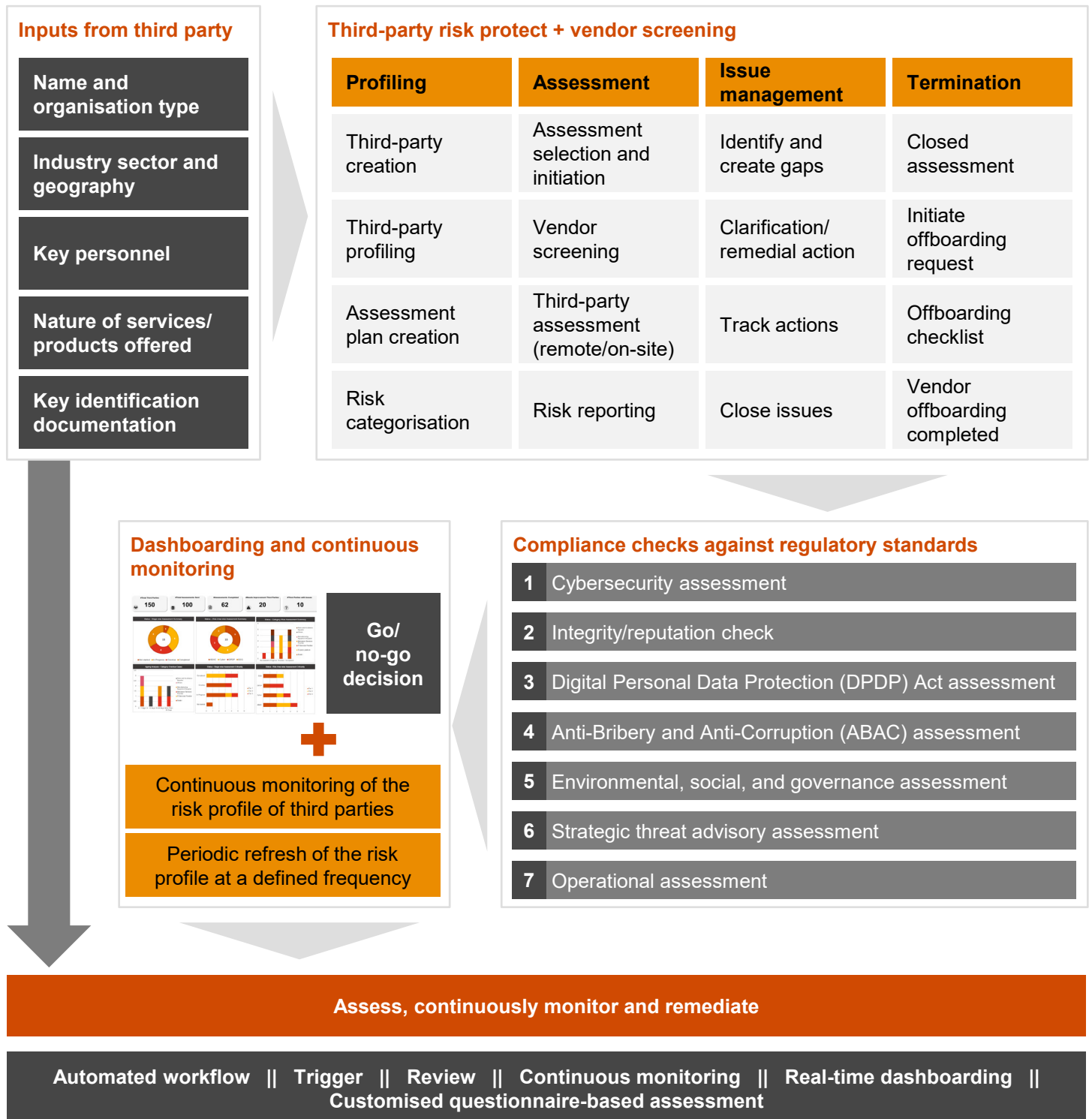
Lack of common and consolidated **performance measures and dashboards** for executive leadership

Real-time reporting capabilities embedded with key performance indicators (**KPIs**), **dashboard** and management information system (**MIS**) reporting to enable effective and timely action and decision-making

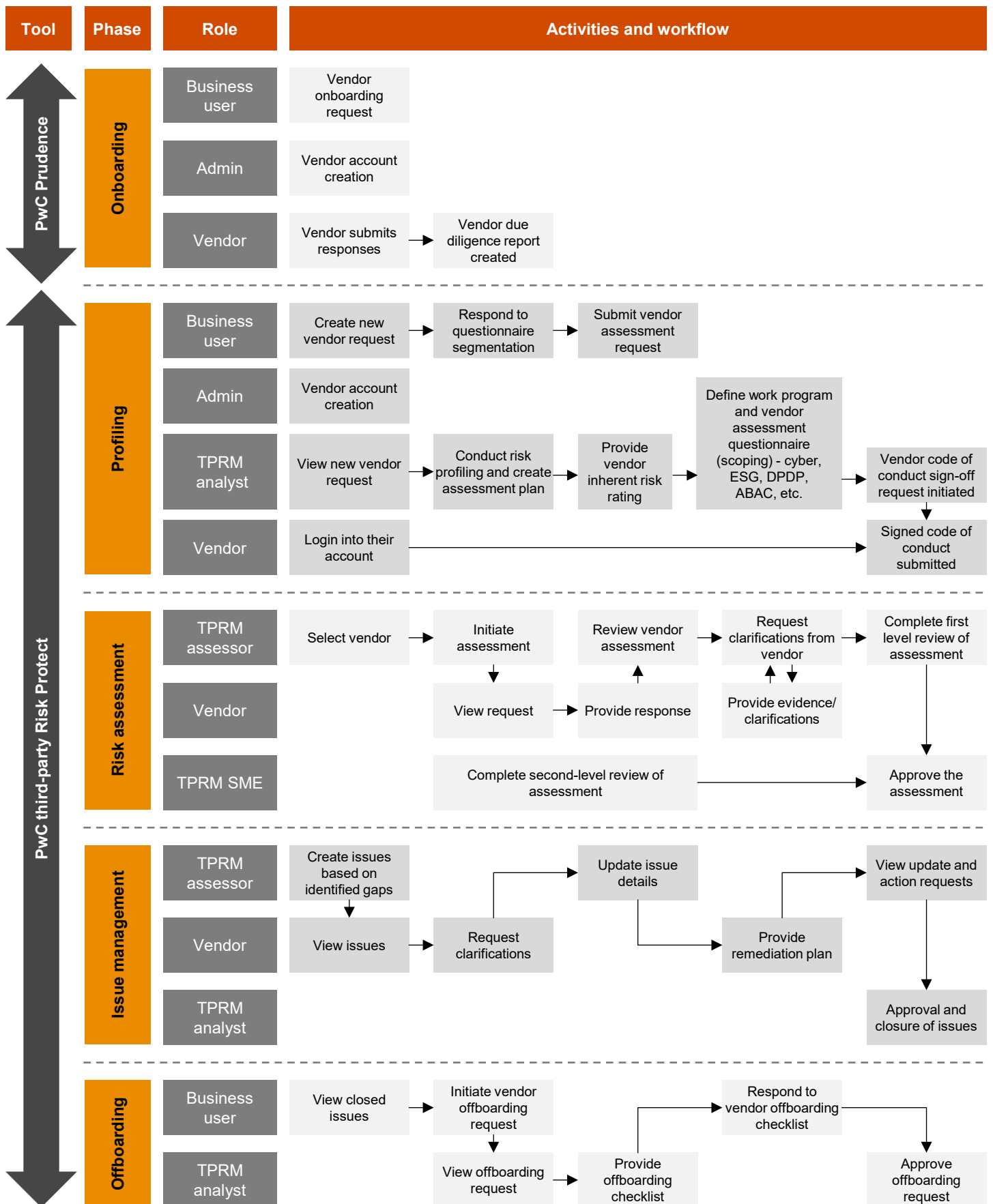
Integrated TPRM solution – PwC's Risk Protect framework

PwC's Risk Protect is a third-party risk management tool which helps clients **automate their third-party onboarding, integrated risk assessment, due diligence and termination** along with value-added capabilities around continuous monitoring, adverse media, risk reporting and contract lifecycle management.

Data sources: Public databases, information provided by third parties, internal transactional data from customer relationship management (CRMs) and enterprise resource planning (ERP) platforms



Risk protect workflow



Features



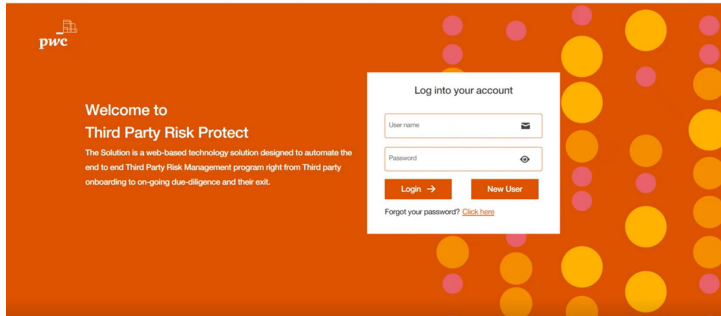
Our approach

01 Integrated framework	02 Automated account creation	03 Assignment of roles	
<ul style="list-style-type: none">• Acts as an integrated framework covering onboarding and offboarding of third-party vendors, conducting risk assessments and remediation on the gaps identified• Risk-based classification of vendors based on service provided, impact and type of data being managed etc.	<ul style="list-style-type: none">• Call-to-action email notifications for role-based responsibilities• Instructions provided over email on the tasks to be performed• Reminder emails in case of overdue assignments• Automated vendor account creation and email notifications	<ul style="list-style-type: none">• Clear assignment of roles and responsibilities• Enables creation of maker-checker• Defined escalation levels	
04 Client SME role included	05 Multiple assessments	06 Vendor due diligence report	
<ul style="list-style-type: none">• New user profile 'Client SME' added to the workflow for second-level review and approval step of the vendor risk assessment• One or more client SMEs can be appointed to review individual assessments across the various risk pillars	<ul style="list-style-type: none">• Can create multiple assessments under a single vendor work programme• Separate questionnaires created for each type of risk assessment recommended such as ABAC, DPDP Act etc.	<ul style="list-style-type: none">• Overall third-party due diligence report summary• Third-party analysis by risk drivers including adverse media, financial, legal etc.• Vendor screening results - dashboard view• Complete risk coverage based on screening results	
07 Inherent and residual risk	08 Issue management	09 Customised dashboards	10 Vendor off-boarding
<ul style="list-style-type: none">• Overall inherent risk rating basis feedback from the business user on nature of services to be provided by the third-party• Overall residual risk rating based on review of the vendor assessment by the Client /TPRM SME• Third-party assessment summary report download option available	<ul style="list-style-type: none">• Identification and creation of gaps• Clarification/remedial action• Tracking actions performed and updated• Tracking both open and closed issues• Open issues ageing analysis• Dashboard view of issues	<ul style="list-style-type: none">• Customisable dashboards – stage, risk areas and third-party categories• Criticality-based assessment reporting• Assessment outcome – risk area, vendor category wise• Ageing analysis of overdue assessments and open issues	<ul style="list-style-type: none">• Allows offboarding a vendor on successful completion of the risk assessment• Reason for offboarding will be provided by the business user• Vendor offboarding checklist will be provided prior to final off-boarding• Status of all offboarded vendors will be visible to the business user

Risk coverage: Cybersecurity risk, ABAC compliance, DPDP Act, ESG compliance

Indicative output and dashboard view

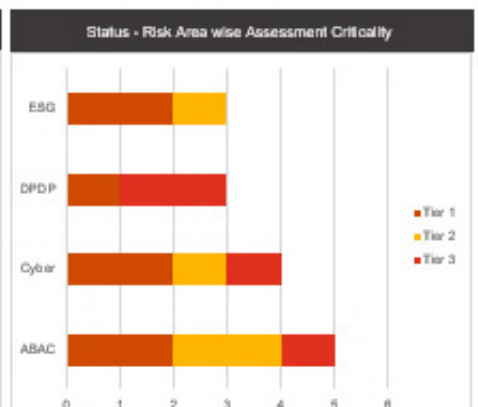
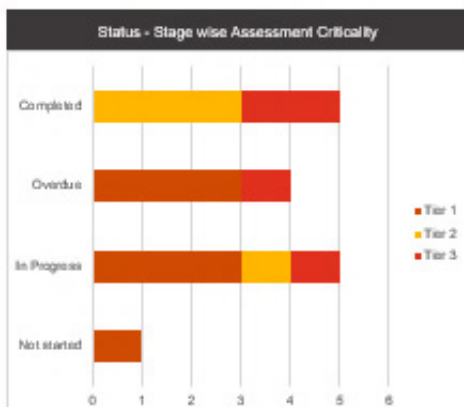
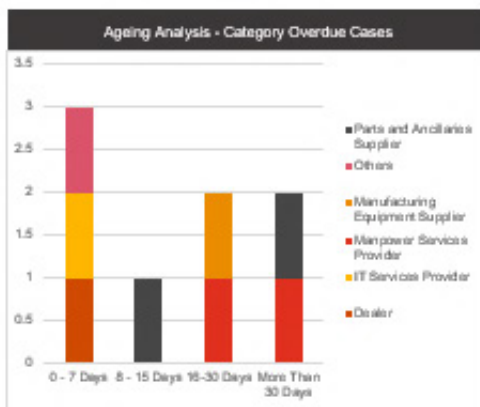
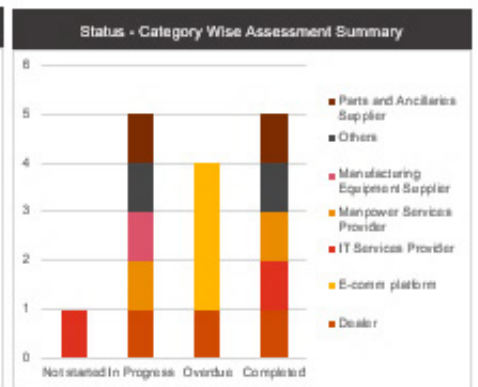
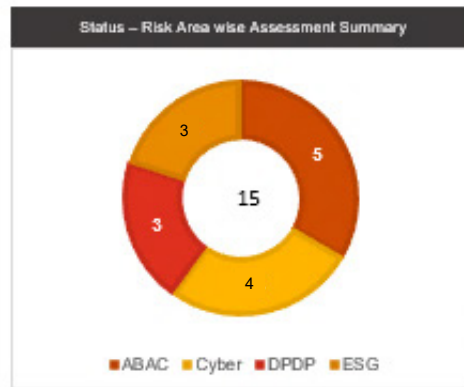
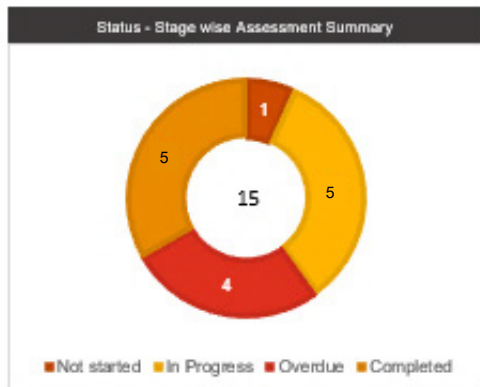
Login page of Risk Protect tool



Assessment and issue management workflow

Issue ID	Status	Third Party Name	Issue Start Date	Issue End Date	Associated Controls	Risk Rating	Action
ISSUE206	Open	Vendor1	2024-07-15	2024-08-15	Does manufacturing equipment provided by you undergo security testing and free from any bug/vulnerabilities?	High	🔍 📄 🗑️
ISSUE207	Close	Vendor1	2024-07-15	2024-08-15	Do you have an Information Security Policy (ISP) documented and approved and reviewed at least annually?	Medium	🔍 📄
ISSUE203	Open	Vendor1	2024-07-19	2024-08-19	Does manufacturing equipment provided by you undergo security testing and free from any bug/vulnerabilities?	High	🔍 📄 🗑️
ISSUE204	Open	Vendor1	2024-07-19	2024-08-19	Do you have an Information Security Policy (ISP) documented and approved and reviewed at least annually?	Medium	🔍 📄 🗑️
ISSUE205	Open	Vendor1	2024-07-22	2024-08-22	Does manufacturing equipment provided by you undergo security testing and free from any bug/vulnerabilities?	High	🔍 📄 🗑️

Near real-time view of company's risk exposure w.r.t. third-party vendors



Supplier risk assessment report scaling

Scale	Rating
95-100	Satisfactory
85-94	Partially Satisfactory
0-84	Needs Improvement

Case studies



Scope of work and approach



PwC value add



Key outcomes

1. Vendor risk assessment for a leading public sector bank in India

- Prepare a framework to evaluate the risk of 250+ IT vendors.
- Conduct a pilot test for 10 suppliers to enhance the framework.
- Conduct onsite assessment.
- Evaluate the risk profile for all vendors, and schedule and conduct regular assessments as per regulatory requirements.
- Perform onsite assessment to review the maturity and mitigation plan.

- The client reached out to understand the compliance with IT outsourcing master direction of RBI and some other compliance requirements of IT vendor risk management.
- We helped the client with the initial thought process through a few discussion rounds.
- We helped the client to set up a vendor risk management programme.

- Evaluation of vendors to identify critical vendors based on risk scores
- Maturity level of the vendor
- Tracking and follow-up to close the identified gaps
- Management reporting for highlighting risky vendors and improvement opportunities

2. Third-party security assessment management services for a leading passenger vehicle manufacturer in India

- Prepare a framework to evaluate the cyber maturity of 500+ suppliers.
- Conduct a pilot for 10 suppliers to enhance the framework.
- Conduct self-assessment and onsite assessment.
- Evaluate the risk scores for all suppliers and identify 100 critical suppliers.
- Perform onsite assessment to review the maturity and mitigation plan.

- The client reached out to understand TPRM.
- We helped client with the initial thought process through a few rounds of discussions.
- We ran a proof of concept (POC) for five suppliers to shape up the scope and expected outcomes.

- Evaluation of suppliers to identify critical suppliers based on risk scores
- Maturity level of the suppliers
- Mitigation plan to close the identified gaps
- Management reporting for highlighting top risks and improvement opportunities

3. Third-party security assessment managed services for an Indian multinational automotive company

- Create and implement a framework for risk ranking/scoring of third parties' cyber risk preparedness status.
- Conduct self-assessment curated according to ISO27001/ISO22301/TISAX for third parties per defined criticality and evaluate the risk scores.
- Perform onsite assessment to review the maturity and mitigation plan.

- The client reached out to conduct third-party risk assessments to identify and address cybersecurity risks and ensure a resilient supply chain.
- We deployed an automated solution with a programme-based approach, providing the client with continual input on its third-party security risk posture.

- Evaluation of third parties to identify critical ones based on the cybersecurity-related risk scores
- Mitigation plan to close the identified gaps
- Tracking third-party responses and providing dashboards to client stakeholders
- Management reporting for highlighting top risks and improvement opportunities



About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with over 360,000 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.

© 2024 PwC. All rights reserved.

Contact us

Puneet Garkhel

Partner and Leader,
TPRM Services

M: +91 98203 20181

E: puneet.garkhel@pwc.com

Anu Purkayastha

Partner,
Risk Consulting

M: +91 98101 48763

E: anu.purkayastha@pwc.com

Mitun Bhattacharjee

Director,
Risk Consulting

M: +91 88794 86112

E: mitun.bhattacharjee@pwc.com



Data Classification: DC0 (Public)

In this document, PwC refers to PricewaterhouseCoopers Private Limited (a limited liability company in India having Corporate Identity Number or CIN : U74140WB1983PTC036093), which is a member firm of PricewaterhouseCoopers International Limited (PwCIL), each member firm of which is a separate legal entity.

This document does not constitute professional advice. The information in this document has been obtained or derived from sources believed by PricewaterhouseCoopers Private Limited (PwCPL) to be reliable but PwCPL does not represent that this information is accurate or complete. Any opinions or estimates contained in this document represent the judgment of PwCPL at this time and are subject to change without notice. Readers of this publication are advised to seek their own professional advice before taking any course of action or decision, for which they are entirely responsible, based on the contents of this publication. PwCPL neither accepts or assumes any responsibility or liability to any reader of this publication in respect of the information contained within it or for any decisions readers may take or decide not to or fail to take.

© 2024 PricewaterhouseCoopers Private Limited. All rights reserved.

PR/October 2024-M&C 41217