uniqus

Third-Party Risk Management (TPRM)

7 common myths

MYTH #1

Myth

A comprehensive TPRM program is only essential for organizations with thousands of third parties.

Reality

Even a single vulnerability in your third-party ecosystem — extending to fourth and nth parties — can jeopardize your entire supply chain. You are only as secure as your weakest link.

How to Address It:

Implement a **“fit-for-purpose”** TPRM program to right-size your efforts and resources and address the risk of an evolving threat landscape.

MYTH #2

Myth

All third parties present the same level of risk.

Reality

Third parties differ significantly in risk exposure, data sensitivity, and operational criticality. A one-size-fits-all approach is ineffective.

How to Address It:

Implement a **risk-based approach** for a more effective and efficient TPRM program.

MYTH #3

Myth

More assessments lead to a stronger TPRM program.

Reality

Many organizations over-engineer TPRM assessments without realizing actual risk reduction.

How to Address It:

Optimize the assessments by adopting a combination of **modernized and intelligent automation techniques** for risk identification.

MYTH #4

Myth

Traditional risk assessments are an essential pillar of effective TPRM.

Reality

In risk posture, the likelihood and impact of an incident are dynamic through a third-party lifecycle. Over-reliance on a one-time snapshot gives the organization a false sense of security.

How to Address It:

Adopt a **data-driven algorithmic approach** combining i**nternal and external parameters** to ensure ongoing visibility and reduce efforts and reliance on manual risk assessments.

MYTH #5

Myth

Rigorous risk assessments lead to a robust TPRM

Reality

Risk mitigation is often overlooked, while risk identification gets hyper attention in the TPRM lifecycle.

How to Address It:

Focus more on **'act' than 'assess'** to reduce the overall risk by utilizing previous issues to address fundamental root causes.

MYTH #6

Myth

TPRM is independent of procurement, IT, or information security.

Reality

Risk mitigation is often overlooked, while risk identification gets hyper attention in the TPRM lifecycle.

How to Address It:

Identify clear **RACI, including the level of involvement throughout the third-party lifecycle management, and use hyper-automation** to reduce coordination debt.

MYTH #7

Myth

Only technology third parties are relevant for TPRM.

Reality

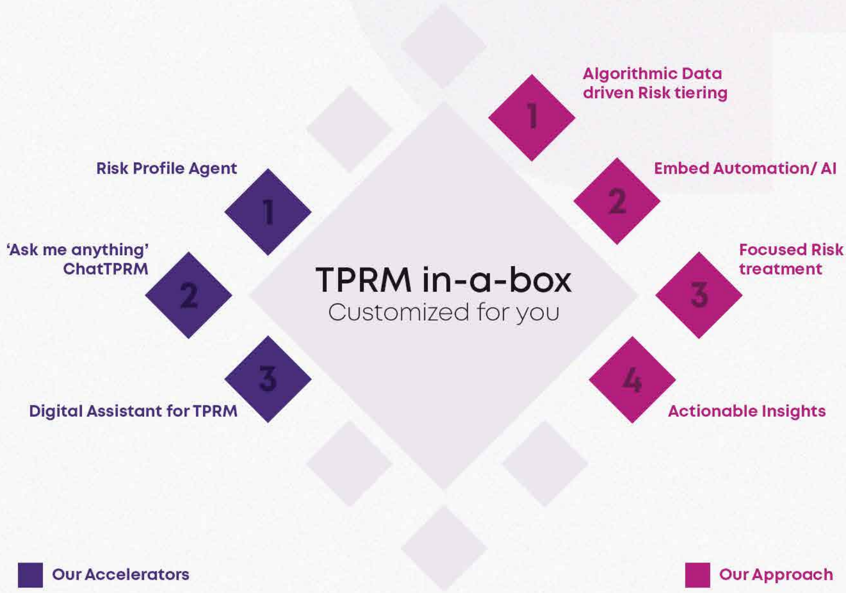
While cybersecurity is a significant concern, TPRM involves compliance, operational risk, financial stability, legal risks, and service continuity.

How to Address It:

Consider all **significant risk areas** (relevant to your organization) and the **100% third-party ecosystem** while defining the building blocks of your TPRM program.

TPRM IN-A-BOX

At Uniqus, we specialize in helping you establish, manage, and optimize a modernized, **fit-for-purpose** Third-Party Risk Management (TPRM) program.



TPRM in-a-box
Customized for you

1 Risk Profile Agent

2 'Ask me anything' ChatTPRM

3 Digital Assistant for TPRM

1 Algorithmic Data driven Risk tiering

2 Embed Automation/ AI

3 Focused Risk treatment

4 Actionable Insights

■ Our Accelerators

■ Our Approach

Foundational Pillars

Visibility:

100% coverage for the third-party ecosystem

Efficiency:

40% efficiency improvement in the first

Consistency:

Improved consistency across the life-cycle

Risk reduction:

Proactive risk reduction for early interventions