KPMG

TPRM challenges continue for financial services institutions

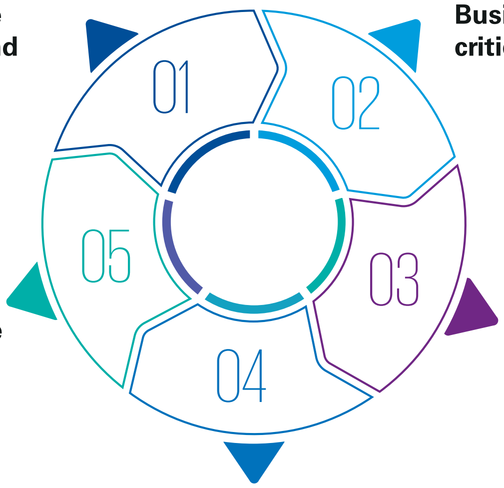
Survey findings offer a wake-up call on the critical need to improve risk management amid soaring cyber threats, geopolitical uncertainty

Financial Services

Third-party risk management (TPRM) has become critical to success in today's complex global business environment. Financial services institutions are now seeing third-party relationships as a key source of competitiveness and growth, making risk-based, enterprise-wide TPRM more important than ever amid increasing threats to business continuity, compliance, reputations and cyber security.

KPMG's *Third-Party Risk Management Outlook 2022* report shows, however, that financial services businesses are struggling with significant TPRM issues that include a lack of skills, insufficient budgets, underperforming technology, evolving regulatory requirements and growing cyber threats. As our latest global research indicates, the outlook for financial services institutions shows no shortage of challenges — and costly disruptions are likely to become more prevalent unless sector businesses take steps to improve TPRM.

Our findings should serve as a wake-up call on the need to reassess and enhance today's TPRM capabilities and operating models. As third-party ecosystems continue to grow in size and complexity, financial services institutions need to approach TPRM maturity in a more consistent and strategic manner that ideally relies on a centralized and refined service model.



Third-party incidents are disrupting operations and damaging reputations

Businesses underestimate the critical need for sound TPRM

Technology is not fulfilling its promise

The challenge of limited resources is here to stay

Financial institutions are struggling to maintain fit-for-purpose TPRM

01 Third-party incidents are disrupting operations and damaging reputations

Missed opportunities to mitigate risk are proving to be a major problem for financial firms, with 72 percent experiencing 'significant disruption, monetary loss or reputational damage as a result of a third-party incident within the last 3 years. Separately, more than half (55 percent) say they have been overbilled by a third party in the last 12 months.

Businesses cite cyber risk (45 percent), financial instability (40 percent) and tech innovation (37 percent) as TPRM risks that have grown most rapidly in recent years. Meanwhile, global regulators are sharpening their focus on operational resilience amid the complex connections supporting countless day-to-day financial transactions that include ATM services, customer loans, bill payments, investments and stock trades.

To keep their services and processes functioning optimally and without interruption, financial services institutions should understand and act on the importance of appropriate third-party assessment and monitoring. They must position themselves to confidently rely on their third-party service providers and, in the event of a disruption, have the capability to rapidly identify and resolve third-party issues.

02 Businesses underestimate the critical need for sound TPRM

Financial services institutions are failing to recognize the value of sound TPRM programs in today's environment and the unfortunate result is a lack of appropriate budgets. TPRM leaders say they are 'frustrated' by their lack of engagement in business continuity amid the typical focus on tactical initiatives over strategic, risk-based programs.

Our survey shows that most financial firms (61 percent) believe TPRM, despite its business-critical role today, is undervalued, with more than half (53 percent) citing insufficient in-house TPRM capabilities to manage risk. More than three-quarters (78 percent) say TPRM should be playing a far more active role in ensuring operational resilience.

With the global pandemic's disruptive impact continuing — and current geo-political events raising the focus on financial crime, sanctions checks and cyber risks — financial firms should focus resources more effectively on appropriate TPRM solutions. Thorough risk assessment among the tens of thousands of third parties typically serving today's global financial institutions is falling short of what is required as firms too often rely on tactical, short-term solutions.

78%

Say TPRM should be playing a far more active role in ensuring operational resilience.

A truly fit-for-purpose TPRM program demands a strategic, integrated approach that provides risk-oversight functions across all business units. Make no mistake — there are no shortcuts in today's dynamic, threat-laden environment.

03 Technology is not fulfilling its promise

While fast-evolving digital technology offers unprecedented capabilities for modern TPRM programs, many financial services organizations say their high hopes for technology are not being met, with many citing their reliance on existing tools that often prove unsatisfactory or burdensome.

59%

Say they are frustrated by the lack of visibility that technology is currently providing around third-party risk.

Fewer than half of all TPRM tasks are currently automated (47 percent), and most firms (59 percent) say they are frustrated by the lack of visibility that technology is currently providing around third-party risk. Key challenges to TPRM transformation cited include data breach concerns (33 percent), integration challenges (30 percent) and a lack of appropriate skills (29 percent).

In many cases, we see firms mistakenly pinning their prospects for success on a single platform — versus an ecosystem of technology and solutions — with the result typically being limited TPRM capabilities and unmet objectives.

Simply put, effective TPRM is not a one-size-fits-all initiative. Progress will likely require financial institutions to better understand what today's technology needs to deliver from a holistic, enterprise-wide perspective.

04 The challenge of limited resources is here to stay

While TPRM's remit is expanding across all risks, domains and third-party types, many sector businesses still lack the depth and breadth of TPRM capabilities needed to effectively manage the significant challenges they are facing.

The number of financial businesses assessing all third parties for environmental risk, for example, is currently 26 percent. While that number is expected to rise to 34 percent within 3 years, it seems clear that financial institutions will likely be hard-pressed to achieve such targets when they already lack the resources needed to manage today's risk environment.

As technology improves, workflow and process automation are expected to significantly enhance efficiency and cost management. In the immediate term, implementing technology with a risk-based approach is the solution to the crucial challenge of resource constraints. This includes aligning the firm's risk appetite with evolving regulatory requirements.

05 Financial institutions are struggling to maintain fit-for-purpose TPRM

Financial institutions say their TPRM programs are 'all too often failing to deliver.' More than half (54 percent) say 'luck' rather than TPRM management has helped them avoid a major third-party incident during the current pandemic.

Nearly two-thirds (63 percent) say they still have a 'long way to go' for their TPRM function to be a true strategic partner to the business, while three quarters (74 percent) say the pandemic's disruptive impact has made clear that an 'overhaul' of their operating model is overdue. We believe our findings should be a wake-up call on the critical need for TPRM leaders and organizations to shift their focus away from tactical initiatives and toward the strategic implementation of risk-based, enterprise-wide programs.

Financial services businesses should 'get back to basics' — managing the journey to TPRM maturity as a priority by defining roles and responsibilities, enhancing third-party assessment, understanding the required end-to-end process, and implementing technology strategically. Ultimately, 'good risk management is good business' in today's dynamic and increasingly complex global environment.

Priorities and next steps toward TPRM maturity

TPRM should be high on financial firm agendas this year as sector businesses grapple with expanding third-party networks, complex operating models, cyber security and reputation threats, evolving regulations and other realities of the post-pandemic era.

Businesses at the early or medium stage of maturity should have need programs that allow them to manage every third party appropriately. Success is expected to require the following steps:

— **Pre-contract to due diligence:** Completing appropriate assessments prior to executing third-party contracts has become indispensable and a key area for improvement.

— **Taking a risk-based approach:** Amid time and resource constraints, financial institutions should focus first on the third parties that impact their critical services, and expand efforts as their TPRM program matures.

— **Ongoing monitoring:** For third parties supporting critical services, financial institutions need to establish thorough and ongoing monitoring programs that help to ensure each third party is consistently meeting expectations.

— **Program governance:** In order to enhance decision making and resolve issues and disruptions in a timely manner, businesses should aim to ensure that all roles and responsibilities are clearly defined.

Businesses at a more-advanced stage of maturity should focus on the following steps to optimize their TPRM programs:

— **Automation:** Forward-looking sector businesses will increasingly automate their end-to-end workflow, using technology to accelerate processes and decision-making while enhancing cost efficiencies.

— **Taking a risk-based approach:** To further streamline the risk tiering of third-party services, tighten the criteria used to define what is 'critical' or 'high' risk, allocate available resources to highest-risk arrangements, and evaluate the need for on-site due diligence measures.

— **Off-boarding and disengagement:** Organizations should understand and define how they can exit a relationship when performance is unsatisfactory, while striving to ensure that customer services remain seamless and uninterrupted.

— **Service-delivery model:** We see an ongoing trend for businesses to establish a unified, enterprise-wide 'center of excellence.' This is an efficient way for organizations with limited resources to cover their third-party network. A unified framework supports consistency across the program, enhanced data quality, and accountability between the central team and relationship owner.

— **Management of fourth parties and affiliates:** In mature programs, fourth parties are no longer out of scope as supplier networks expand. Businesses therefore should have appropriate controls that include contract documentation and consistent alignment with existing TPRM program requirements.

Contacts

David Hicks
Global Forensic and Financial Crime Transformation Lead
KPMG International
E: david.hicks@kpmg.co.uk

Alexander Geschonneck
Global Third-Party Risk Management Lead, KPMG International, and Partner
KPMG in Germany
E: ageschonneck@kpmg.com

Greg Matthews
Third-Party Risk Management Americas Lead and Partner
KPMG in the US
E: gmatthews1@kpmg.com

Jon Dowie
Third-Party Risk Management Europe, Middle East and Africa Lead and Partner
KPMG in the UK
E: jon.dowie@kpmg.co.uk

Gavin Rosettenstein
Third-Party Risk Management Asia-Pacific Lead and Partner
KPMG Australia
E: gavin1@kpmg.com.au

home.kpmg/socialmedia

Designed by Evalueserve.

Publication name: TPRM challenges continue for financial services institutions
Publication number: 137978-G
Publication date: May 2022