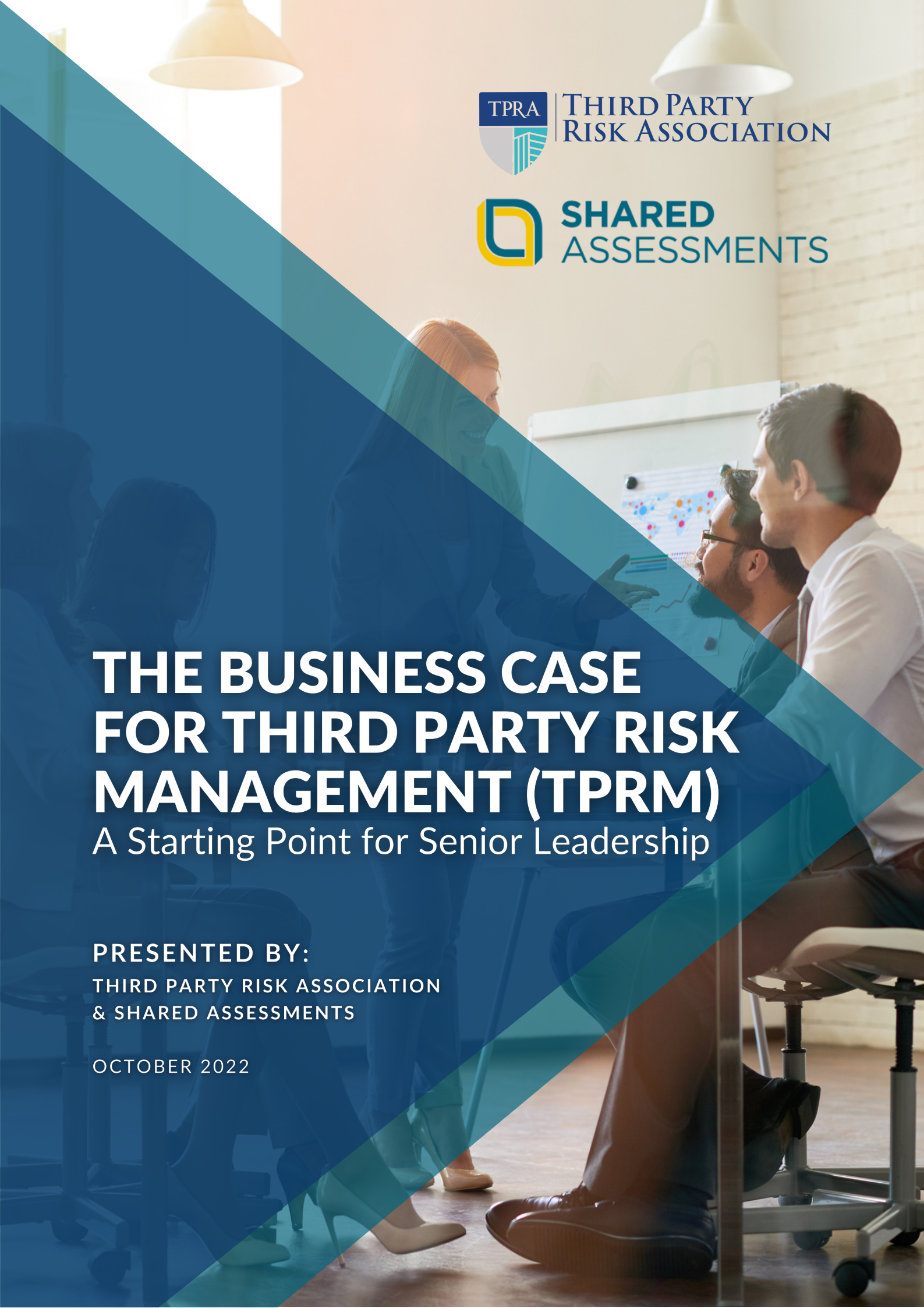

TPRA | THIRD PARTY RISK ASSOCIATION

SHARED ASSESSMENTS

THE BUSINESS CASE FOR THIRD PARTY RISK MANAGEMENT (TPRM)

A Starting Point for Senior Leadership

PRESENTED BY:

THIRD PARTY RISK ASSOCIATION
& SHARED ASSESSMENTS

OCTOBER 2022

I. WHAT IS THIRD PARTY RISK MANAGEMENT?

To achieve their goals, businesses today increasingly use **third parties** to support all corporate and revenue-generating services, including banking, call centers, consulting, facility management, financial reporting, human resources, technology development and infrastructure.

Third Party is broadly defined as any entity that provides products and/or services to an organization, whether or not a contract is in place or monies are exchanged (e.g., Affiliates, Subsidiaries, Consultants, Contractors, Sub-Contractors, Vendors, Service and Solution Providers, Fourth parties, and more).

While third parties extend the available resources and expertise of an organization, too often the consideration and management of their associated **risks** is not commensurate with the opportunities these parties offer.

Risk is the possibility of an adverse impact on an organization's data, financials, operations, reputation, or other business objectives, as a direct or indirect result of a failure in process, resource, and/or technology.
Risk = Likelihood of Event x Impact of Event

To address these more effectively, boards, senior executives, and risk leaders at firms need to ensure **third party risk management (TPRM)** is launched and supported as an enterprise function to protect the organization, its clients, and its employees from a range of potential risks, including compliance, cyber, financial, operational, strategic, technological, as well as reputational.

Third Party Risk Management (TPRM) is the framework that consists of policies and procedures, **controls**, and oversight; established to identify and address the direct and/or indirect risks presented to an organization by their third parties.

Control is a process and/or activity used to monitor, review, or address a specific risk.

To create an effective business case for launching and operating a Third Party Risk Management program, a firm's senior leadership (preferably with Board support) must first agree on the need for such a program, share realistic expectations around the messaging and minimum investment involved, and agree upon the measurable outcomes expected from the program investment.

THE NEED: WHY IS A TPRM PROGRAM IMPORTANT?

Any organization needs a TPRM program to ensure third parties are operating securely and effectively, comply with regulatory requirements and other industry standards, and participate in regular monitoring to identify and manage the risks that could affect their business, clients, or both. Without those measures, a firm cannot consistently or meaningfully understand and mitigate risks related to third party access to your sensitive data, internal systems, and/or outsourced functions needed to support business operations. Remember: risk is never transferred to a third party if a process is outsourced. In fact, an organization's threat surface is merely expanded when engaging a third party, and your firm always retains a fiduciary obligation to protect the information and other assets associated with your organization and your clients. As a result, organizations can face major financial, legal, and reputational repercussions without a TPRM program. With such a program, a firm can evaluate the potential financial risk from your third parties (via business impact analysis) in a consistent, repeatable manner across business and risk functions, helping the firm focus on highest probable loss events, potential regulatory fines, and other impacts from engaging external parties. For example, the Consumer Financial Protection Bureau (CFPB) has imposed fines totaling $530 million for some major banks due to the risk their third parties created (such as deceptive practices).

II. PLANNING YOUR TPRM INVESTMENT: ESSENTIAL PROGRAM FEATURES

To ensure TPRM Program success, we recommend several essential program features to consider during the planning phase to ensure adequate support, broad implementation, and a suitable framework for your organization.

1

LEADERSHIP SUPPORT

Senior leadership and even Board support are essential to ensure any TPRM function starts with a clear mandate. Absent that support (by setting the right "tone at the top"), a firm is unlikely to achieve uniform and timely adoption across all of their business and risk functions. That leadership support also requires sufficient funding; measurable, realistic program milestones; and an expectation of regular progress reporting that is shared up to senior leadership and even Board level.

2

ENTERPRISE-WIDE IMPLEMENTATION

Since third parties generally support all aspects of a company's operations and revenue-generating activities, the scope of their risks ultimately mirrors every aspect of your organization. As a result, only enterprise-wide implementation will ensure a TPRM program covers all relevant business risks for a firm. In addition, firms need to establish a Risk Appetite for their material risks (e.g., compliance, cyber, financial, operational) to establish a foundation for the TPRM program. Note that there is not one value or appetite for Third Party Risk, because these parties pose a range of risks, not all equal, so an organization's appetite for each form of risk must align with the appetite you extend to your third parties (e.g., Low Appetite for Compliance Risk, Medium Appetite for Operational Risk). Without defined and documented risk appetites, any TPRM program risk scoring and prioritization will remain arbitrary and misaligned with your business.

Risk Appetite is the level of risk an organization is willing to accept before requiring any action to reduce the related risk. These are uniquely defined by the types of risk each organization needs to manage based on the nature of its business. Since no business can operate without risk, a risk appetite must always exist (e.g., High, Medium, or Low) and is never zero or null.

3

TPRM FRAMEWORK

Along with leadership support and enterprise-wide implementation driven by defined risk appetites, a TPRM framework should establish a firm's general requirements for the following:

- **Third-Party Onboarding** – whether establishing new business relationships or new services under existing relationships
- **Due Diligence** – when required at onboarding and the expectations for updated or recurring reviews
- **Ongoing Oversight** – criteria for regular oversight, whether based on risk, service type, or degree of outsourcing
- **Disengagement/Termination** – expectations for when and how to terminate individual services or entire business relationships

This framework should establish the key objectives for each stage of the TPRM lifecycle but not necessarily the exact timeframes, service levels, or other operational metrics intended for standards or even operating procedures. The goal is to establish effective TPRM governance objectives.

4

BUDGET CONSIDERATIONS

Establishing basic or even aspirational objectives under a TPRM framework requires a realistic alignment with available budgets to support risk operations. For example, if a TPRM framework requires diligence for all higher risk third parties pre-contract execution and ongoing monitoring for all post-contract execution, a commensurate budget and staff levels are necessary to achieve those objectives.

Budget considerations include the following:

- **Resources** – current and future employees and/or contractors.
- **Operations** – any cost associated with daily tasks and running the business.
- **Maturity Model** – process enhancements required and what is needed to get there.
- **Travel** – costs associated with onsite visits
- **Training** – fees for conferences, trainings, and certifications to ensure maintenance of knowledgeable & skilled professionals that are appraised of risk trends.
- **Tools** – budget for TPRM program tools, but include estimated cost savings a tool(s) will bring by automating certain processes.

5

RISK COMMITTEE

The firm's Risk Committee or equivalent should establish the thresholds for risk escalation and risk acceptance reporting. The TPRM or broader Enterprise Risk Management (ERM) framework should establish the nature and frequency of reporting to a firm's Risk Committee, whether leadership, Board level, or both.

6

TRANSPARENCY & COMMUNICATION

Transparency and communication are key when developing, implementing, and maintaining any TPRM program. Third parties touch almost every department within your organization. Therefore, all stakeholders need to be familiar with TPRM program policies and procedures, as well as their role within the program. Business owners need to understand they are the owners of their third party's risk and that the TPRM program's role is to support their risk-based decisions related to any third party.

7

REPORTING

Ensure you establish measurable, specific, and relevant metrics for your program. Metrics should guide the development and execution of your program, as well as inform stakeholders of the overall risk landscape related to your organization's third parties. Reporting should be tailored to specific target audiences to ensure they make data-driven decisions after reviewing the information. Below is an example of target groups that should receive regular TPRM program updates.

- **Board** – receive the overall health of the TPRM program, as well as updates on the higher-risk third parties and risk mitigation strategies.
- **Executives** – receive the risk ratings of third parties within each department, as well as updates on risk-mitigation strategies for higher-risk third parties.
- **Risk Committee(s)** - receive risk ratings of third parties within each department, updates on risk-mitigation strategies, escalations, and risk requiring acceptance.
- **Business/Relationship Owners** – receive updates on the due diligence efforts for their third parties, as well as assessment outcomes.
- **Other Stakeholders** *(such as Compliance Teams)* – receive data on specific risks posed to the firm (such as regulatory/compliance risk).
- **TPRM Managers** – receive updates on program maturity, resource allocation, risk mitigation efforts, process exceptions, escalations, and any risks requiring business acceptance.

BENCHMARKING & CONTINUOUS IMPROVEMENT

Benchmarking with other TPRM programs and thought leaders is key when developing and maintaining your TPRM program. The value you receive from benchmarking against other programs, frameworks, and thought leaders includes, but is not limited to the below.

Leverage What Already Exists

Allows you to leverage what has already been developed so that you are not "re-creating the wheel." There are several tools and techniques available that will help guide you in setting up and launching your program.

Maintain Flexibility

Continually enhance due diligence efforts to maintain flexibility and consider risk trends, as well as new assessment domains that should be incorporated because of regulations, threats, and/or vulnerabilities.

Grow With Your Business

Consider the growth of your organization. As your business grows, adds products, or even operates in new jurisdictions, prepare to change how you benchmark to ensure you evaluate your program to your latest peers for proper comparisons. Are you in a new tier of peers and comparing apples to apples?

Validate Established Activities

Compare and validate your established program activities. It is best practice to regularly perform a gap analysis against your program requirements compared to established frameworks and best practice thought leadership. This ensures you continually align your program with said frameworks and, in turn, build assurance around, formalize, and sustain your program objectives.

DEFINING EXPECTED PROGRAM OUTCOMES: RETURN ON INVESTMENT

Now that we know what TPRM is and the steps needed to launch or mature a related program, let's look at what the return on investment includes when you implement a TPRM program:

1

VISIBILITY INTO YOUR THIRD PARTY RISK

The program will assist with the build-out and maintenance of an inventory of your organization's third parties. This is harder than most people realize and can take months or even years to perfect, but you cannot manage what you cannot count or measure. The program should also consider third parties your organization may/may not pay, accept click through agreements from, as well as those operating via unique business relationships that are outside of procurement or normal payment processes. This program should also help you to create organizational definitions and criteria for each third-party relationship (such as software supplier, broker, facility maintenance, etc.).

2

FURTHER DEFINE THE POTENTIAL IMPACT THIRD PARTIES POSE TO YOUR ORGANIZATION

The program will run all your third parties through an inherent risk questionnaire (IRQ) to determine the highest-level risk rating for each before evaluating any controls. This should then drive your organization's due diligence efforts. Keep in mind the importance of each risk domain covered by the IRQ is driven by your organization's Risk Appetite.

3

THIRD PARTY DUE DILIGENCE & CONTINUOUS MONITORING

The program will assess third party risk on a regular basis to ensure contract terms, business obligations, legal and regulatory requirements, and performance expectations are met. The program should consider reviewing other risk domains outside of cybersecurity (such as financial, operational, strategic, and regulatory risk).

An effective TPRM program is essential to ensure third parties are operating securely and effectively, monitored regularly, and the risks related to managing your data and any outsourced processes are mitigated and align to your organization's expectations.

4

RISK MITIGATION EFFORTS

The entire purpose of a TPRM program is to identify and mitigate third party risk. Therefore, it is crucial the program validates findings, works with your third parties to create remediation plans, and follows up on risk mitigation efforts. As a result of a strong TPRM program, you should expect to see a reduction in residual risk associated with your third parties, thereby mitigating their potential impact on your organization.

5

REGULATORY COMPLIANCE

Regulatory compliance has been a stable item on many board agendas but lately has become the number one topic within organizations, largely due to the increase of regulations around your organization's relationships with third parties. There are a variety of reasons behind this focus, but the main drivers are related to the threat landscape growing in complexity, momentum of digital transformation, political and social unrest, as well as responses to the global pandemic. The regulatory risks your third parties do not address can present both reputational and financial risk for your own firm if your organization's name comes up as purchasing services from said third party should an issue arise. As a result, regulatory agencies are mandating you understand the risks associated with doing business with your third parties. Ensuring your third party is complying with pertinent regulations may result in a reduction of regulatory fines on your organization, ensure they are operating with integrity, and actively preventing attempts at bribery, corruption, and other threats.

6

OPERATIONAL RESILIENCY

As a part of the TPRM program, your organization should gain an understanding of how your third parties will operate in the event of a disruption or other disaster. You should also understand how your third party's disaster recovery efforts will affect you (i.e., when you will receive communication, when services will be back up, what data you will have access to in the event of data recovery efforts, and how/when your third party will notify you and/or your customers in the event of an incident and/or breach).

Collectively, these program investments and expected outcomes will ensure your firm's TPRM program achieves the key objectives most commonly expected by Boards, regulators, and clients.

Third Party Risk Association

Furthering the Profession of Third Party Risk Through Knowledge Sharing & Networking

Address
P.O. Box 824
Ankeny, Iowa 50021
USA

Email
info@tprassociation.org

Website
www.tprassociation.org

LinkedIn
Third Party Risk Association (TPRA) - Third Party Risk Management

Instagram
@tprassociation

YouTube Channel
Third Party Risk Association

Shared Assessments

Shared Assessments is a Member-Driven Organization Delivering Secure and Resilient Third-Party Partnerships

Address
1751 Calle Medico, Suite N
Santa Fe, NM 87505

Phone
(505) 466-6434

Website
https://sharedassessments.org

LinkedIn
Shared Assessments

Twitter
@SA_Program