THIRD PARTY
RISK ASSOCIATION

February's Member Meeting

Julie Gaiaschi, CEO & Co-Founder

For your awareness, this call is being recorded

TPRA | THIRD PARTY RISK ASSOCIATION

AGENDA

- Opening Remarks
- Presentation/Roundtable: “The Business Case for TPRM”
  - Value of a TPRM Business Case
  - What is TPRM?
  - Need for a TPRM Program
  - Essential Program Features
  - Benchmarking & Continuous Improvement Efforts
  - Return on Investment
- TPRM “Tool Talk” Demo Presented by RiskRecon
- Closing Remarks

TPRA | THIRD PARTY RISK ASSOCIATION

Opening Remarks:

- **2/14 -** Retail & Manufacturing Special Interest Call @ 10 – 11 AM CST
- **2/14** – Technology Special Interest Call @ 1 to 2 PM CST
- **2/16 -** Focus Group Call @ 10 AM CST – Due Diligence Questionnaires
- **2/16** – Finance Special Interest Call @ 1 PM – 2 PM CST
- **2/21** – Healthcare/Insurance Special Interest Call @ 10 – 11 AM CST
- **2/21** – Women in TPRM Call @ 1 – 2 PM CST
- **3/3** – Q1 Practitioner Network Event @ 1- 2 PM CST

TPRA | THIRD PARTY RISK ASSOCIATION

Opening Remarks:

- **YouTube** Channel – Subscribe to Third Party Risk Association
  - New Video Alert: “What is Third Party Risk Management?”
- **Slack Space Forum** – Join under “Member Services” using the “Slack Forum” link.
- Join our **LinkedIn Page** to view upcoming events and promotional opportunities.
- Follow our **Instagram Page** for Monday memes, behind the scene look at conference planning, and event updates.

THIRD PARTY RISK ROUNDUP

April 24 - 26, 2023

Nashville Marriott at Vanderbilt University

2555 West End Ave

Nashville, Tennessee

www.thirdpartyriskroundup.org

Discount Code:
"FG100" for $100 off any ticket price.

Included:

- TPRA Bag & T-Shirt & Registration (Premium Members Receive VIP Surprises)
- Breakfast, Lunch, & Snacks throughout Days 2 & 3
- Two Country-Themed Network Events w/ Drinks & Appetizers (Live Singers for One)
- All Keynotes, Break Outs (Three Tracks to Choose From), Panels, Demos, & Peer Roundtables
- Sponsor Booths (TPRM Tools)
- Fun Games & Great Raffle Prizes (Including a $500 Delta Gift Card)

Agenda (Example Topics):

- Keynote: Big 4 Panel Discussion on TPRM Today & Tomorrow (Will include Deloitte, EY, KPMG, & PwC)
- Building a Resilient Supply Chain
- Panel: Avoiding Blind Spots in TPRM
- The Importance of Relationships During Onboarding and Ongoing Monitoring
- Cloud Metadata Abuse by Threat Actors
- Security Trends: Results of 1000 Security Assessments
- Panel: Practitioner Perspectives on Continuous Monitoring Success
- Delivering Value w/ Cyber Loss & Data Breach
- Unlocking TPRM Program Potential through Governance & Metrics
- Three Roundtables: TPRM Essentials & Better Practices, Operational Risk & Resilience, & Innovation & Automation

TPRA | THIRD PARTY RISK ASSOCIATION

CERTIFICATION PROGRAM NOW OPEN

Submit your application today!

REGISTER

Check Our Website

WWW.TPRASSOCIATION.ORG/TPRA-CERTIFICATIONS

TPRA | THIRD PARTY RISK ASSOCIATION

Third Party Cyber Risk Assessor© (TPCRA©) Certification

The TPCRA Certification is a specialized qualification designation to confirm your understanding and skill in the assessment of third party cyber security controls and processes, as well as validate your competency in the creation, execution, and management of third party cyber risk assessments.

Examination: Scheduled at a **PearsonVue** location near you on the date and time you select. (Exam emails will begin to go out **March 20, 2023**.)

Domains:

- Cybersecurity and TPRM Basics
- Pre-Contract Due Diligence
- Continuous Monitoring
- Physical Validation
- Disengagement
- Cloud Due Diligence
- Reporting and Analytics

Training Dates:

- Private Training: February 15 – 16 @ 9 AM – 4 PM CT
- Virtual via Zoom: March 6 - 7 @ 9 AM - 4 PM CT each day
- Virtual via Zoom: March 27 - 30 @ 5 - 8 PM CT each night
- In-Person @ Nashville, TN: April 24 @ 3 - 6 PM CT, April 25 @ 9 AM - 4 PM CT, and April 26 @ 9 AM - 12 PM CT (at in-person conference)

TPRA | THIRD PARTY RISK ASSOCIATION

The Business Case for TPRM

Source: TPRA & Shared Assessment's whitepaper on **"The Business Case for TPRM: A Starting Point for Senior Leadership"** available within the TPRA Blog site.

TPRA | THIRD PARTY RISK ASSOCIATION

What is the Value of a TPRM Business Case?

- Provides basic guidance for Senior Executives and Board Members to encourage them either to launch new or mature legacy third-party risk programs.
- Ensures a firm's senior leadership (preferably with Board support) first agrees on the need for a TPRM program, shares realistic expectations around the messaging and minimum investment involved, and agrees upon the measurable outcomes expected from the program investment.
- Shares what regulators and clients routinely expect from such programs: the need to improve their ability to protect their firms, their clients, and the related assets they are working to safeguard.
- Assists in obtaining leadership's commitment to and budget for TPRM programs.

TPRA | THIRD PARTY RISK ASSOCIATION

What Does a Business Case Consist Of?

- Explain What is TPRM (to include common definitions)
- Need for a TPRM Program
- Essential Program Features
- Benchmarking & Continuous Improvement Efforts
- Return on Investment

TPRA | THIRD PARTY RISK ASSOCIATION

What is Third Party Risk Management?

- **Third Party** – Broadly defined to include all entities that can or do provide products and/or services to an organization regardless as to whether a contract is in place or monies are exchanged. Such entities can include, but not be limited to: Affiliates, Subsidiaries, Consultants, Contractors, Sub-Contractors, Vendors, Service and Solution Providers, Fourth parties, and more.
- **Third Party Risk** – 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 an organization's third party.

Risk = Impact of an Event x Likelihood Event Will Occur

- **Control** – A process and/or activity used to monitor, review, and/or address a specific risk.
- **TPRM** – Is the framework that consists of policies and procedures, controls, and oversight; established to identify and address risks imposed upon an organization by their third parties.

TPRA | THIRD PARTY RISK ASSOCIATION

Why is TPRM 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.

TPRA | THIRD PARTY RISK ASSOCIATION

Essential Program Features:

- **Leadership Support:** Senior leadership and even Board support are essential to ensure any TPRM function starts with a clear mandate. Absent that support, 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, as well as the Board.
- **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.
- **Risk Appetite:** Defined as the level of risk an organization is willing to accept before requiring any action to reduce the related risk. 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. Without defined and documented risk appetites, any TPRM program risk scoring and prioritization will remain arbitrary and misaligned with your business.

TPRA | THIRD PARTY RISK ASSOCIATION

Essential Program Features:

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:

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.

TPRA | THIRD PARTY RISK ASSOCIATION

Essential Program Features:

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.

Note: TPRA Practitioner Call around TPRM Budgeting is scheduled for September.

TPRA | THIRD PARTY RISK ASSOCIATION

Essential Program Features:

- **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.
- **Transparency & Communication:** 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.

TPRA | THIRD PARTY RISK ASSOCIATION

Essential Program Features:

Reporting: Ensures 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 "recreating 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?
- **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.

TPRA | THIRD PARTY RISK ASSOCIATION

Return on Investment

- **Visibility Into 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.).
- **Further Define 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.

TPRA | THIRD PARTY RISK ASSOCIATION

Return on Investment

- **Establish 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).
- **Establish 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.

TPRA | THIRD PARTY RISK ASSOCIATION

Return on Investment

- **Ensure 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. The regulatory risks your third parties do not address can present both reputational and financial risk for your own firm. 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.
- **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).

TPRA | THIRD PARTY RISK ASSOCIATION

Summary

- 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.
- 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.
- 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.

TPRA | THIRD PARTY RISK ASSOCIATION

Questions?

TPRA | THIRD PARTY RISK ASSOCIATION

Next Meeting: Thursday, March 9, 2023 @ 10 to 11:30 AM CST

Topic – "Assessing Inherent & Residual Risk"
(IRQ & Risk-Based Due Diligence Efforts) + "Tool Talk" Demo

TPRA | THIRD PARTY RISK ASSOCIATION

TOOL TALK

WITH

riskrecon

mastercard

TPRA | THIRD PARTY RISK ASSOCIATION

TPRM Lifecycle

- **Planning and Oversight** provides an organization with the foundation to build upon and properly support their overall program.
- **Pre-Contract Due Diligence** ensures the organization performs due diligence, commensurate with the level of inherent risk, to determine if the organization should proceed with a specific third party relationship and prior to signing a contract. This phase assists with determining if a third party meets business needs in context of the risk presented.
- **Contract Review** ensures the organization documents relationship expectations in an agreement that can be upheld in a court of law. It also ensures risks noted within the due diligence process can be addressed within contractual clauses.
- **Continuous Monitoring** requires the organization to assess third party risk on a continual basis to ensure contract terms, business obligations, legal and regulatory requirements, and performance expectations are met.
- **Disengagement** ensures the organization is able to transition away from a third party with minimal impact should the relationship end due to contract expiration or when adverse/unplanned conditions are met.
- **Continuous Program Improvement** is an ongoing activity which seeks to enhance the organization's TPRM program as third party risk management guidance, trends, and techniques are realized.