THIRD PARTY
RISK ASSOCIATION

June's Member Meeting

Julie Gaiaschi, CEO & Co-Founder

For your awareness, this call is being recorded

TPRA | THIRD PARTY RISK ASSOCIATION

AGENDA

- Opening Remarks
- Roundtable: “Integrated Business Processes”
  - Collaboration w/ Internal Stakeholders
  - Risk-aware Culture
  - Business Owner Buy-In
  - TPRM Program Expectations
  - Reporting & Escalations
- Closing Remarks
- “TPRM Tool Talk” with Aravo

TPRA | THIRD PARTY RISK ASSOCIATION

Opening Remarks:

- **6/12 to 6/15 – TPCRA Virtual Training** @ 5 – 8 PM Central
- **6/15 Focus Group Call** @ 10 AM Central – Due Diligence Questionnaires
- **6/20 – Women in TPRM Call** @ 1 to 2 PM Central
- **6/23 Special Interest Call: Big 4** @ 11:30 AM Central (Invite Only)
- **YouTube** Channel – Subscribe to Third Party Risk Association
- **Slack Space Forum** – Join under "Member Services" using the "Slack Forum" link.
- Join our **LinkedIn, Facebook, and Instagram Pages** to view upcoming events, Monday memes, and TPRM quick hits!
- TPRA **Swag Shop** is now OPEN! Visit www.tprassociation.org/swag.

TPRA | THIRD PARTY RISK ASSOCIATION

https://www.tprassociation.org/2023-virtual-conference

Save the Date - Fall Virtual Conference

- **Theme:** Operational Risk & Resilience
- **Date:** Wednesday, September 27th @ 9 AM to 4 PM Central
- **Cost**: Free for TPRA Members & Non-Members
- **CPE**: 6 Hours of Continuing Professional Education (CPE) credits
- **Proposed Topics**: Proactive Due Diligence, Threat Intelligence, Incident Response, Review of Certificate of Insurance, Enhanced Financial Reviews, Incorporating Emerging Risks into the Assessment Process, Onsite Visits, Findings & Follow Up, Contracting for a Resilient Relationship, etc.
- **Call for Speakers/Sponsors OPEN!**
- **Registration OPEN!**

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.

Domains:

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

Training Dates:

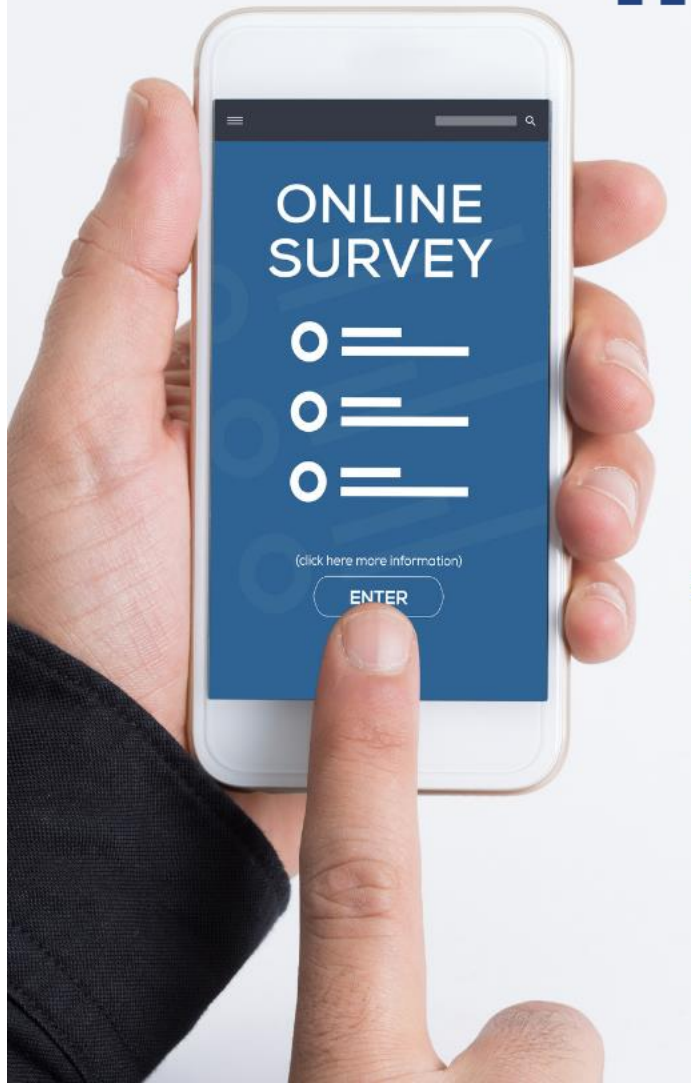
- Virtual: **June 12 – 15** @ 5 PM - 8 PM CT each night
- Virtual: **July 25 – 26** @ 8 AM - 3 PM CT each day
- **On-Demand**: Coming Soon!

TPRA | THIRD PARTY RISK ASSOCIATION

TPRM Compensation & Hiring Survey

Take the Survey!

For those that take the survey today, will be entered into a drawing for a $50 Amazon Gift Card!



This survey aims to obtain information from TPRM practitioners on the topic of hiring practices & compensation. Results from the survey will be analyzed, summarized, & distributed in a report to those wishing to receive it.

Take the Survey!

TPRA | THIRD PARTY RISK ASSOCIATION

Roundtable: Integrated Business Processes

TPRA | THIRD PARTY RISK ASSOCIATION

Why is TPRM Process Integration Important?

- When bringing in a new third party, the end goal is to optimize third party products/services being offered to your organization, as well as support the business owners leveraging said products/services. Ultimately, third parties support business owner's day-to-day business objectives.
- But with the use of third parties comes additional risk to the organization.
- Ensuring TPRM is integrated into the organization effectively will assist with reducing third party risk while ensuring business objectives are met.
- The challenges with integration is usually speed to market, as well as the amount of time and work it takes to mitigate third party risk.

TPRA | THIRD PARTY RISK ASSOCIATION

Collaboration w/ Internal Stakeholders:

- When first starting out a TPRM program, it is important to look at what is needed in order to evaluate and mitigate risk. Usually, it is a better understanding of the controls a third party has in place, as well as an evaluation of specific controls. In order to do that, a contract must be in place that allows for said assessment of controls.
- This usually means you will need to work with Legal, Procurement, Vendor Management, and other various departments to ensure you are evaluating controls before the contract is signed, ensuring appropriate language is in the contract, and evaluating controls on a continuous basis after the contract is signed.
- In order to ensure everyone is on the same page with regards to a TPRM program, your organization should have a risk-aware culture. But what does this really look like?

TPRA | THIRD PARTY RISK ASSOCIATION

Risk-Aware Culture:

- Executive Support
- Business and Stakeholder Champions
- Risk Committee where key stakeholders have a seat at the table
- Strong TPRM policy and procedures
- Roles & Responsibilities are communicated and agreed to
- Good reporting is in place and tailored to target audiences
- Periodic review of the TPRM program occurs
- If automating, key stakeholders evaluate tools
- Findings roll into a central repository and are regularly reviewed
- An escalation process is in place, as is an incident response program

TPRA | THIRD PARTY RISK ASSOCIATION

Business Owner Buy-In:

- Transparency & Communication are key
  - Training & Education on the program and the business' role
  - Understand business goals and objectives (which includes identifying key projects and timelines)
  - Understand the relationship that exists between the third party and the business.
  - Identifying what the business needs and incorporating into your activities.
- Only ask for what is needed. (Ensure your TPRM program is risk-based.) Also ensure you are only reaching out a few times. If you aren't getting what you need, then jump on a call.
- Create an exit strategy for third party relationships to ensure the business can move on as quickly as possible should a termination occur.
- Let the business know you are there for them, to support their decisions. Ultimately, they own the risk and you will provide your services to help identify and mitigate said risk. (Service Catalogue)

TPRA | THIRD PARTY RISK ASSOCIATION

TPRM Program Expectations:

- Regularly review TPRM program expectations with key stakeholders, business owners, and third parties. This ensures everyone is on the same page and knows what is happening.
- Items to be reviewed are:
  - Program expectations for each target audience,
  - Assessments conducted for each tier/third party category and why,
  - Evidence items required and timelines for obtaining said items,
  - Findings validation, follow up, and closure processes,
  - Escalation procedures, and
  - Reporting activities (what types of reports each target audience will receive)
- It is also important to discuss with the Board and Executives where the program is at from a maturity perspective and next steps to be implemented to get to the next level of maturity, as well as the return on investment for getting to that next level.

TPRA | THIRD PARTY RISK ASSOCIATION

Escalations & Reporting:

- Define out escalation paths for your program to ensure you know when to escalate and who should receive escalations. Also determine if certain escalations will require certain Legal involvement.
- Escalations may lead to the enactment of the incident response plan.
- It is important to also know who to escalate to or receive escalations from, on the third party's side. You may want to include in your contract notification requirements for escalations and incidents.
- With regards to 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 risk landscape related to your organization's third parties. Reporting should be tailored to specific target audiences to ensure they make better, data-driven decisions after reviewing the information.

TPRA | THIRD PARTY RISK ASSOCIATION

Reporting:

- Board of Directors – Overall health of the TPRM program, the impact of and mitigation activities for higher-risk (inherent & residual) third parties, emerging risks and threats, and regulatory matters. Overall, the Board should receive a comprehensive understanding of the organization's third-party risk management program, including its effectiveness, key risks, and strategies for mitigating those risks.
- Program Sponsors (Executives) – Receive the risk ratings for third parties assessed, as well as updates on risk-mitigation strategies for higher-risk third parties.
- Risk Committee(s) - Receive risk ratings for third parties assessed, as well as updates on risk-mitigation strategies, escalations, and risks requiring acceptance. Also receive updates on emerging risks and threats, as well as regulatory matters.

TPRA | THIRD PARTY RISK ASSOCIATION

Reporting:

- TPRM Program Owner/Facilitator – Receive updates on program maturity, resource allocation, risk mitigation efforts, process exceptions, escalations, and any risks requiring business acceptance.
- Business/Relationship Owners – Receive updates on third party due diligence efforts, as well as assessment outcomes.
- Key Stakeholders (such as Compliance Teams) – Receive data on specific risks posed to the organization (such as regulatory/compliance risk).
- Third Parties – Receive updates on TPRM program expectations, findings identified (for validation and to set remediation plans), and compliance requirements. You may also choose to send security incidents that may affect their operations (if they become known to you). Please work with your Legal team to determine if there are liability considerations as it relates to distribution.

TPRA | THIRD PARTY RISK ASSOCIATION

Questions?

TPRA | THIRD PARTY RISK ASSOCIATION

Next Meeting: Thursday, July 13, 2023 @ 10 to 11 AM CST

Topic – Panel: **“Keeping Pace with Regulatory Change”**

TPRA | THIRD PARTY RISK ASSOCIATION

TOOL TALK

WITH

ARAVO