THIRD PARTY
RISK ASSOCIATION

May'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: “Nth Party Reviews”
  - Identification
  - Assessment Techniques
  - Contract Requirements
  - Findings & Follow Up
- No TPRM “Tool Talk” Today
- Closing Remarks

TPRA | THIRD PARTY RISK ASSOCIATION

Opening Remarks:

- **5/16** – Special Interest Call: Healthcare & Health Insurance @ 10 to 11 AM CST
- **5/16** – Women in TPRM Call @ 1 to 2 PM CST
- **5/18** – Special Interest Call: Finance @ 1 to 2 PM CST
- **6/2** – Q2 Practitioner Network Event @ 1 to 2 PM CST
- **YouTube** Channel – Subscribe to Third Party Risk Association
- **Slack Space Forum** – Join under "Member Services" using the "Slack Forum" link.
- Join our **Facebook**, **LinkedIn & Instagram pages** to view upcoming events and promotional opportunities.

TPRA | THIRD PARTY RISK ASSOCIATION

Save the Date - Fall Virtual Conference

- **Theme:** Operational Risk & Resilience
- **Date:** Wednesday, October 11th @ 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** – Opening Up Soon!

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 is now LIVE.)

Domains:

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

Training Dates:

- Virtual: **May 15 – 18** @ 8 AM - 11 AM CT each day
- Virtual: **June 12 – 15** @ 5 PM - 8 PM CT each night
- Virtual: **July 18 – 19** @ 8 AM - 3 PM CT each day
- On Demand Training: **Coming Soon!**

TPRA | THIRD PARTY RISK ASSOCIATION

Roundtable: Nth Party Reviews

TPRA | THIRD PARTY RISK ASSOCIATION

What is an Nth Party?

- Your third party's third, fourth, or fifth party.
- It is an organization you do not directly contract with but could have a significant impact on the products/services your third party is providing to you.
- Depending on the nature of the contracted services, nth parties could have your data or directly contact your customers.
- Because of the data they may house and/or services they perform, they could affect your organization's bottom line and/or reputation should something negative occur.

TPRA | THIRD PARTY RISK ASSOCIATION

Identification:

- Each organization should identify what a “material” subcontract is based on their own organization’s risk appetite. (Data, contact with customers, critical infrastructure, material supply chain, etc.)
- Request material current and future subcontractors from your third parties (should be in contract).
- Leverage TPRM tools to perform nth party discovery activities.
- Review SOC 2, Type II reports (which usually state some material sub-contractors).
- Request and review data flow diagrams to see where data is being sent.
- Leverage IT teams to help identify (as they can usually obtain the information).

TPRA | THIRD PARTY RISK ASSOCIATION

Assessment Techniques:

- At a minimum, you need to understand the who, what, where, and for what purpose your third party contracts with other organizations.
- Review your third party's TPRM program to determine if nth parties are sufficiently assessed.
- May request your third party provide to their fourth party your security questionnaire and have them complete it.
- Request documents and evidence from your third party on their material nth parties (i.e., vulnerability scans and pen test results if they will house your data).
- You may even request to have a conversation with the nth party (with your third party present) on specific issues should you not get all of the information necessary to determine their controls environment.

TPRA | THIRD PARTY RISK ASSOCIATION

Contract Requirements

The following slides do not represent legal advice. If you have specific questions concerning specific circumstances, please consult your attorney.

TPRA | THIRD PARTY RISK ASSOCIATION

Contract Requirements:

- Contracts should require your third party to communicate to you current, material third parties, as well as future third parties. They should also communicate when third party relationships change (such as when they are moving to a new third party or when they are terminating third party relationships).
- Note within the contract the type of information required… such as name, location, services, and data accessed per subcontractor.
- Should also have a clause that states your third party will have a TPRM program in place that ensures the security and operational effectiveness of their third parties. (Example of clause on next screen.)
- Can also note within the clause any specific evidence you would like on the fourth party (may also state “will allow the participation of a conversation with the fourth party from time to time if deemed necessary”).
- Should also have a non-compliance clause within the agreement should your third party not comply with any of the above clauses. (Such as withholding monies or performing additional due diligence.)

TPRA | THIRD PARTY RISK ASSOCIATION

Contract Requirements:

- “Vendor must implement and maintain a process: (i) to review and conduct risk assessments on a regular basis (at least annually), on subcontractors that have access to Company Data, commensurate with the amount and type of Company Data to which the subcontractor has access; and (ii) to ensure each subcontractor has the ability to comply, and does in fact comply, with the obligations of this Agreement, including this [Security Policy], with respect to the protection of Company Data. Vendor must have appropriate contracts in place with all of its subcontractors that will have access to Company Data prior to services being initiated that include provisions consistent with this [Security Policy] and [that provision we just talked about] of this Agreement. Contracts with such subcontractors shall include, at minimum, [stuff we really care about]”
- Source: Nyemaster Law Firm

TPRA | THIRD PARTY RISK ASSOCIATION

Findings & Follow Up:

- Request information on any issues that came out of your third party's TPRM due diligence related to nth parties and ask how those issues are being remediated.
- Based on the information you've obtained about the nth party, perform your own conclusions on their controls environment and follow up on any questions you may have.
- If high risks are discovered, request to have a conversation with the nth party to validate and clarify information. If this is not allowed, then ask the third party to.
- If the fourth party is looking to be a high risk, then request your third party move you off their services. If not possible, then escalate within your own organization to determine next steps (such as moving away from your third party).

TPRA | THIRD PARTY RISK ASSOCIATION

Questions?

TPRA | THIRD PARTY RISK ASSOCIATION

Next Meeting: Thursday, June 8, 2023 @ 10 to 11:30 AM CST

Topic – Roundtable: **“Integrated Business Processes”** - Enabling the Business while Mitigating Risk + TPRM Tool Talk