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
- Roundtable: Third Party Engagement
  - Third Party Buy-In
  - Third Party Response Time
  - Assessment Evidence Provided
  - Assessment & Findings Validation
  - Third Party Expectations
- Closing Remarks

TPRA | THIRD PARTY RISK ASSOCIATION

Update: 30 tickets left, as well as only 6 speaker slots remaining!

the art of Third Party Risk

Be a part of the highly anticipated event of the year!

- Premiere event for **only 120 registrants.**
- April 18th – 20th, 2022
- AT&T Conference Center & Hotel in Austin, TX
- Early Bird Pricing (Happening Now) - $200 Members, $300 Non-Members, & $1,000 Vendors
- If you are interested in speaking and/or sponsoring, please email Julie@tprassociation.org.

For more information & to purchase your ticket, visit www.artofthirdpartyrisk.org

EXPERIENCE networking events and meet third party risk experts and industry leaders

ENGAGE with service providers that can help you enhance your program!

DISCOVER best practices for third party risk management and elevate your program to the next level

TPRA | THIRD PARTY RISK ASSOCIATION

Opening Remarks:

- **YouTube** Channel - TPRM Explained: "TPRM Maturity vs. Associated Value"
- **Slack Space Forum** – Join under "Member Services" using the "Slack Forum" link.
- Join our **LinkedIn Page** to view upcoming events and promotional opportunities.
- **Registration** for upcoming events has now switched to **Zoom**. Easier to register and allows you to download an Outlook calendar invite.

February Events	Date	Time (CST)
Volunteer Interest Call	2/15/2022	10 AM - 10:30 AM
Focus Group Call	2/24/2022	10 AM - 11 AM

TPRA | THIRD PARTY RISK ASSOCIATION

Roundtable: Third Party Engagement

Allows organizations to monitor and assess the risk posed by third parties to identify where it exceeds organizational risk appetite. It also allows organizations to make risk-informed decisions and reduce the risk posed by third parties to an acceptable level.

- Third Party Buy-In
- Third Party Response Time
- Assessment Evidence Provided
- Assessment & Findings Validation
- Third Party Expectations

TPRA | THIRD PARTY RISK ASSOCIATION

Third Party Buy-In:

- During RFP phase, communicate TPRM program processes & activities. Also communicate third party expectations and timelines.
- Set up reoccurring meetings with the third party and the business to work through assessments and ongoing monitoring activities.
- Educate new third party account representatives, as well as new business owners on program activities and expectations.
- Communicate escalation procedures up front so the third party is aware of what would be considered an item that will be escalated.
- Request contacts for not only SMEs that can complete certain assessments, but also if escalation is required (Compliance, Legal, Privacy, CEO, CISO).
- May also want to create a limited assessment should the longer assessments go well.

TPRA | THIRD PARTY RISK ASSOCIATION

Third Party Response Time:

- During the first of the year or when a new third party is on-boarded, provide a list of assessments to be performed, as well as an evidence list and tie target dates to each item. Regularly follow up on the items.
- When certain evidence items cannot be provided, work with the vendor to determine evidence that can be obtained (screen share, jumping on a call and talking through a process, reviewing secondary controls, etc.).
- If working through a re-assessment, share with the third party what was provided the previous year and ask if there are any changes that need to be made.
- Set up an annual meeting with the business to review how the product/service is being leveraged to determine if there are any changes to the use of the product/service, data sent, or other risk-based changes were made. Send out an annual questionnaire to the third party to ask if there have been any recent changes to policies/procedures, leadership, product/services offered, sub-contractors, offshore resources, etc.

TPRA | THIRD PARTY RISK ASSOCIATION

Assessment Evidence Provided:

- When setting up your TPRM program, determine your organization's risk appetite (what you are willing/ not willing to accept from a risk perspective).
- For more important (key) controls, ensure you obtain evidence from the third party to validate controls are in place and operating effectively.
- Determine what evidence is ideal and what is acceptable for said key controls.
- Provide a list of evidence items to the third party in advance and tie target dates to each item for when it will be provided.
- Once you validate evidence, discuss with the third party when evidence is not sufficient. Use your list of acceptable evidence items to determine if another evidence option can be obtained.
- If sufficient evidence cannot be obtained, inform the third party of why it is important and necessary to obtain. Also enlist the assistance of the business owner to escalate to others within the third party organization.
- Issue a finding if the evidence cannot be obtained and determine if risk acceptance is necessary. Ensure it is noted within the contract during renewal of it is a key item.

TPRA | THIRD PARTY RISK ASSOCIATION

Assessment Evidence Provided (Examples):

- Penetration test
- Independent attestation – Includes SOC 2, Type II reports.
- Policies and procedures
- Proof of key controls to evidence effectiveness
- Vulnerability report/evidence of patching
- Continuous monitoring report
- Financials
- DR/BC plans and testing
- Employee counts – Includes key person dependency and any significant changes that have occurred.
- Network diagram – Includes cloud architecture and a data flow diagram.
- Background checks – Includes policies and samples of actual background checks.
- Employee access reviews
- Training – Includes broadscale and specific/targeted training.
- Model risk – Includes validation of models.
- Negative news

TPRA | THIRD PARTY RISK ASSOCIATION

Assessment & Findings Validation:

- Ensure your assessment approach is risk-based, as in you are not asking the third party to perform an assessment with the inherent and/or residual risk is low or the assessment is not applicable.
- If the third party is providing a critical service, may want to work through an onsite assessment to gain a better “feel” for responses you are receiving vs. what is actually happening at third party facilities.
- If you do discover a finding, communicate it to the third party in a timely manner so they can validate the issue and gain a better understanding on why it is important to your organization.
- Provide validated findings to the third party in a document, along with seeded remediation plans (should not be specific but set an expectation with regards to what you are looking for). Allow the third party to draft the remediation plan and tie a reasonable target date to it.

TPRA | THIRD PARTY RISK ASSOCIATION

Third Party Expectations:

- Document third party expectations for your TPRM program and ensure incorporated into contracts:
  - Responding to assessments and questionnaires,
  - Providing evidence (may want to call out specific evidence items),
  - Working with your organization on validation of findings,
  - Working with your organization in creating remediation plans and target dates,
  - Ensure your organization is incorporated into the third party DR and Incident Response plans,
  - Communicate non-compliance triggers when information is not obtained and/or findings are not being remediated in an acceptable or timely manner.
- Communication and Collaboration is key. Let your third parties know they are an extension of your own security program and that you learn from them just as much as they may learn from you.

TPRA | THIRD PARTY RISK ASSOCIATION

Next Meeting: Thursday, March 10th from 10 to 11:00 AM CST

Topic: Recertification & Re-Assessments (Cycles, Assessment Types, Questionnaires, Evidence Collected)

Thank you for joining!