THIRD PARTY
RISK ASSOCIATION

March's Member Meeting

Julie Gaiaschi, CEO & Co-Founder

For your awareness, this call is being recorded

THIRD PARTY RISK ASSOCIATION

AGENDA

- Opening Remarks
- Roundtable: Recertification and Reassessments
  - Assessment Types
  - Questionnaires
  - Evidence Collected
  - Assessment Cycles
- Closing Remarks

TPRA | THIRD PARTY RISK ASSOCIATION

Update: Limited tickets remaining.
Hotel rate was extended to April 1st.

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 (Ends 3/18) - $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 – Subscribe to Third Party Risk Association
- **Slack Space Forum** – Join under "Member Services" using the "Slack Forum" link.
- Join our **LinkedIn Page** to view upcoming events and promotional opportunities.
- **Quarterly Special Interest Calls -** If you are in the Finance & Insurance, Healthcare & Insurance, Retail, and/or Technology industries, join us each quarter for our industry-specific special interest calls. The next calls are April 19th and 21st.
- **Quarterly Network Event -** Join us each quarter for a fun and informal network event! Thanks to those that attended last Friday's event. Our next event is June 3rd.

TPRA | THIRD PARTY RISK ASSOCIATION

Roundtable: Recertification & Reassessment

- Inherent Risk Questionnaire (IRQ) usually drives the due diligence process. Recertify IRQ to determine if responses remain the same or if the IRQ should be updated. Recertify vendor profile, to include location of services.
- Based on re-reviewed IRQ responses, determine which assessments are in and out of scope. Many assessments previously performed are most likely still in scope (unless the way in which products/services leveraged have materially changed).
- Re-review previously completed assessments to determine 1) if there are any outstanding follow up items (evidence wasn't provided, findings are still in the remediation process, certain questions were not answered) and 2) what the previous risk score was related to the assessment.
- Based off re-review and scheduled assessment cycle times, may perform a limited assessment or a full assessment.
- Inherent and residual risk should also play into the reassessment process.

THIRD PARTY RISK ASSOCIATION

Assessment Types:

- Information Security Risk Assessment – May include application, data, and network security, Software Development Lifecycle (LDLC), and Service Organization Controls (SOC) 2, Type II report reviews.
- Privacy Impact Assessment – Includes data management and regulations.
- Financial Assessment – Involves the viability of an organization.
- Disaster Recovery and Business Continuity (DR/BC) – Covers techniques and processes for continuing business performance following a disaster.
- Physical Access Controls – Determines potential threats to properties, objects, or individuals and the controls to mitigate said risk.
- Regulatory Assessment – Examples include Payment Card Industry (PCI), HIPAA, and Gaming.
- Negative News Monitoring – Monitoring media content, looking for any existing media concerning a third party, signaling a potential threat—whether reputational or security—to your organization.
- Passive Monitoring – Risk Rating / Intelligence tools
- Third/Fourth Party Profile/Assessment – Reviewing the controls in place for your third party's suppliers.
- Offshore Reviews – Reviewing the controls in place to mitigate additional risk an offshore location may pose to your organization.

TPRA | THIRD PARTY RISK ASSOCIATION

Questionnaires:

- Inherent Risk Questionnaire (usually answered by the business)
- Information Security Assessment (to include cloud-specific questions)
- Financial Viability Questionnaire
- DR/BC Plan & Testing Questionnaire
- Privacy Questionnaire
- Offshore Questionnaire
- Sub-contractor Questionnaire
- Operational Resiliency Questionnaire
- Compliance and Regulatory Questionnaire
- Environmental, Social, Governance Questionnaire
- Changes in Doing Business Questionnaire
- Industry-specific Questionnaire
- HR & Hiring Practices Questionnaire

Evidence Collected:

- There may be evidence items you want to obtain each year to ensure controls are operating effectively (ex. Penetration test results, vulnerability scans, patch management efforts, access reports).
- There may be times when a full assessment is not required if specific evidence items can be obtained for testing.
- There may also be times when you want an independent test performed for key controls to ensure it is thoroughly reviewed.
- Certain changes in the relationship and/or way in which the product/service is leveraged may trigger ad hoc reviews. Such examples include, but are not limited to, change in location of services, change in risk rating (risk rating/intelligence tool), change in ownership of the third party, change in product/service (may now be cloud-based vs. on premise), change in data sent/stored, change in contract clauses, and an event or incident occurring.

TPRA | THIRD PARTY RISK ASSOCIATION

Evidence Collected (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 Cycles:

- May want to base assessment cycles off inherent and/or residual risk ratings.
- Example: Information Security Review
  - If Inherent Risk is High and IRQ notes the third party hosts or has access to Confidential data, then the review is IN-SCOPE.
  - Third Party completed an Information Security review the prior year and the results were favorable; thereby, making the residual risk low.

		Residual Risk		
Inherent Risk	**Information Security Review**	**High**	**Medium**	**Low**
	High	Every Year – Full	Every Year – Limited	Every Other Year - Limited
	Medium	Every Year – Full	Every Other Year - Limited	Every Three Years - Full
	Low	Not Required	Not Required	Not Required

THIRD PARTY RISK ASSOCIATION

Next Meeting: Thursday, April 14th from 10 to 11:00 AM CST

Topic: Panel discussion on Automating TPRM (Effective Use of Tools, Implementation, & Trends)

Thank you for joining!